Exhibit 1

US009001985B2

(12) **United States Patent**
Cox et al.

(10) **Patent No.: US 9,001,985 B2**
(45) **Date of Patent: Apr. 7, 2015**

(54) METHOD OF AND SYSTEM FOR DISCOVERING AND REPORTING TRUSTWORTHINESS AND CREDIBILITY OF CALLING PARTY NUMBER INFORMATION

(75) Inventors: **Patrick M. Cox**, Newberg, OR (US); **Richard J. Greene**, Portland, OR (US); **Joseph H. Bockelman**, Springboro, OH (US); **Shreyas Saitawdekar**, Portland, OR (US)

(73) Assignee: **TrustIP, Inc.**, Portland, OR (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **13/567,592**

(22) Filed: **Aug. 6, 2012**

(65) **Prior Publication Data**

US 2012/0294435 A1 Nov. 22, 2012

Related U.S. Application Data

(63) Continuation of application No. 12/783,405, filed on May 19, 2010, now Pat. No. 8,238,532.

(60) Provisional application No. 61/179,629, filed on May 19, 2009.

(51) **Int. Cl.**

H04M 15/00	(2006.01)
H04M 17/00	(2006.01)
H04M 15/06	(2006.01)
H04M 17/02	(2006.01)

(52) **U.S. Cl.**

CPC ***H04M 15/06*** (2013.01); ***H04M 15/47*** (2013.01); ***H04M 15/83*** (2013.01); ***H04M 15/8351*** (2013.01); ***H04M 17/02*** (2013.01)

(58) **Field of Classification Search**

CPC H04M 1/57; H04M 1/663; H04M 1/667; H04M 1/82; H04M 15/47; H04M 15/48; H04M 2550/60; H06Q 20/00; H06Q 20/382; H06Q 20/3825; H06Q 20/389; H06Q 20/40; H06Q 20/401; H06Q 20/4014; H06Q 20/4016; H06Q 40/025

USPC 379/114.14, 121.01, 143.01, 144.03, 379/127.01, 127.02; 705/7.28, 38, 64, 67, 705/74, 75

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,699,416	A	12/1997	Atkins	
5,963,625	A *	10/1999	Kawecki et al.	379/127.01
6,307,926	B1	10/2001	Barton et al.	
6,947,532	B1 *	9/2005	Marchand et al.	379/114.14
6,975,708	B1 *	12/2005	Scherer	379/88.22
7,653,188	B2 *	1/2010	Kloberdans et al.	379/145
7,912,192	B2 *	3/2011	Kealy et al.	379/114.14
2003/0225686	A1 *	12/2003	Mollett et al.	705/38
2007/0271339	A1	11/2007	Katz	
2008/0084975	A1 *	4/2008	Schwartz	379/88.22
2009/0187508	A1 *	7/2009	Placide	705/72
2010/0275011	A1 *	10/2010	Horgan et al.	713/155

* cited by examiner

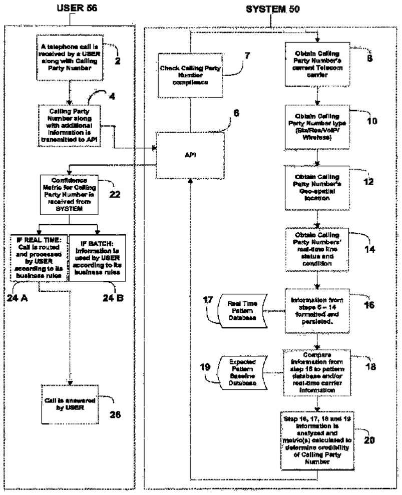
Primary Examiner — Binh Tieu

(74) *Attorney, Agent, or Firm* — Sterne, Kessler, Goldstein & Fox P.L.L.C.

(57) ABSTRACT

A method of and system for discovering and reporting the trustworthiness and credibility of calling party number information, such as Automatic Number Identification (ANI) or Calling Number Identification (Caller ID) information, or for inbound telephone calls. The disclosed method entails the use of real time telephone network status and signaling, network data, locally stored data, and predictive analytics. Practice of the disclosed method is neither detectable by nor intrusive to the calling party, and the method can be implemented into existing enterprise, telecommunications, and information service infrastructures.

22 Claims, 2 Drawing Sheets


USER 56
SYSTEM 50
A telephone call is received by a USER along with Calling Party Number
2
Calling Party Number along with additional information is transmitted to API
4
Check Calling Party Number compliance
7
API
6
Obtain Calling Party Number's current Telecom carrier
8
Obtain Calling Party Number type (Biz/Res/VoIP/Wireless)
10
Obtain Calling Party Number's Geo-spatial location
12
Obtain Calling Party Numbers' real-time line status and condition
14
Information from steps 6 – 14 formatted and persisted.
16
Real Time Pattern Database
17
Compare information from step 16 to pattern database and/or real-time carrier information
18
Expected Pattern Baseline Database
19
Step 16, 17, 18 and 19 information is analyzed and metric(s) calculated to determine credibility of Calling Party Number
20
Confidence Metric for Calling Party Number is received from SYSTEM
22
IF REAL TIME: Call is routed and processed by USER according to its business rules
24 A
IF BATCH: Information is used by USER according to its business rules
24 B
Call is answered by USER
26

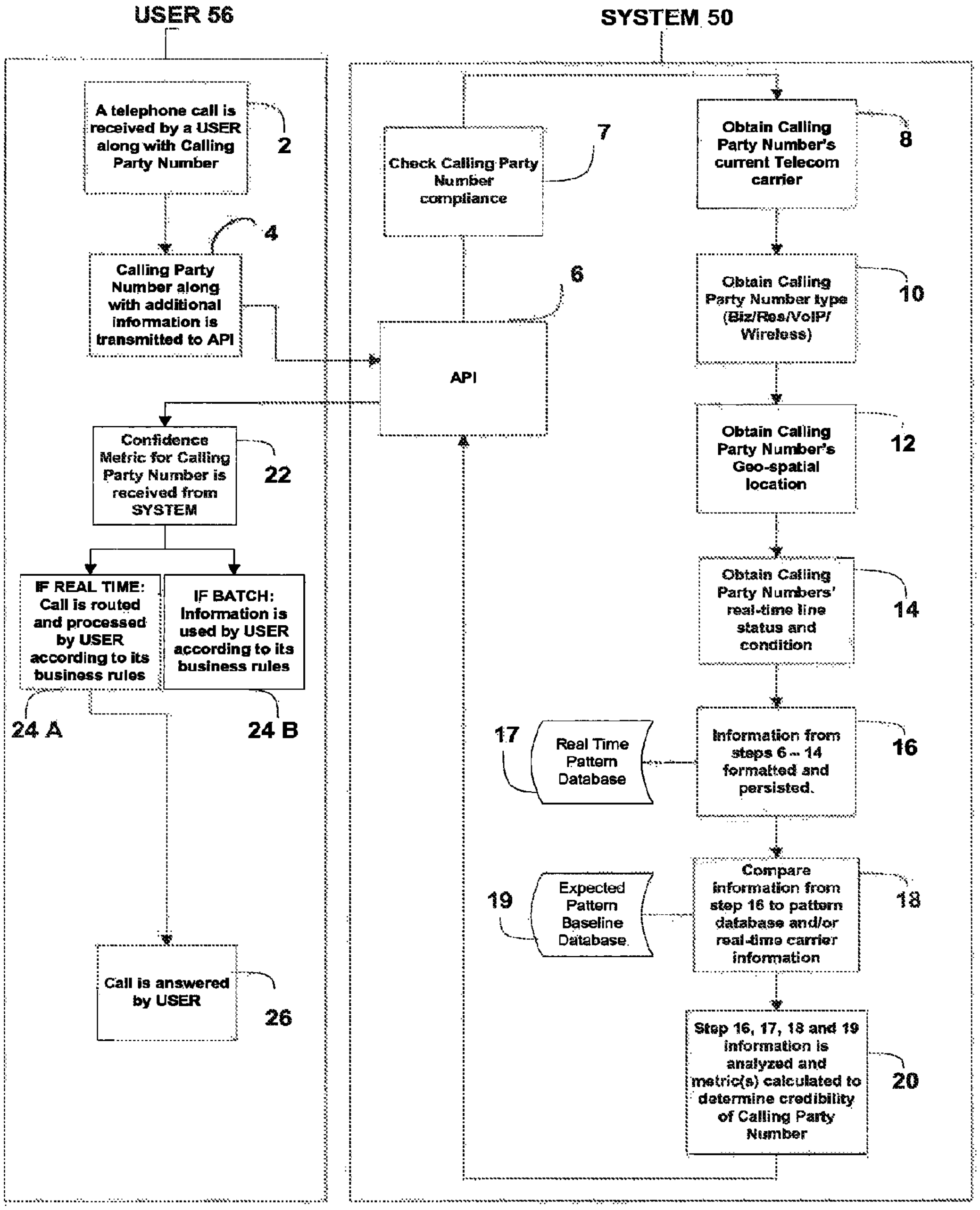

USER 56
SYSTEM 50
A telephone call is received by a USER along with Calling Party Number
2
Calling Party Number along with additional information is transmitted to API
4
Confidence Metric for Calling Party Number is received from SYSTEM
22
IF REAL TIME: Call is routed and processed by USER according to its business rules
IF BATCH: Information is used by USER according to its business rules
24 A
24 B
Call is answered by USER
26
Check Calling Party Number compliance
7
API
6
Obtain Calling Party Number's current Telecom carrier
8
Obtain Calling Party Number type (Biz/Res/VoIP/ Wireless)
10
Obtain Calling Party Number's Geo-spatial location
12
Obtain Calling Party Numbers' real-time line status and condition
14
Real Time Pattern Database
17
Information from steps 6 – 14 formatted and persisted.
16
Expected Pattern Baseline Database
19
Compare information from step 16 to pattern database and/or real-time carrier information
18
Step 16, 17, 18 and 19 information is analyzed and metric(s) calculated to determine credibility of Calling Party Number
20

FIG. 1

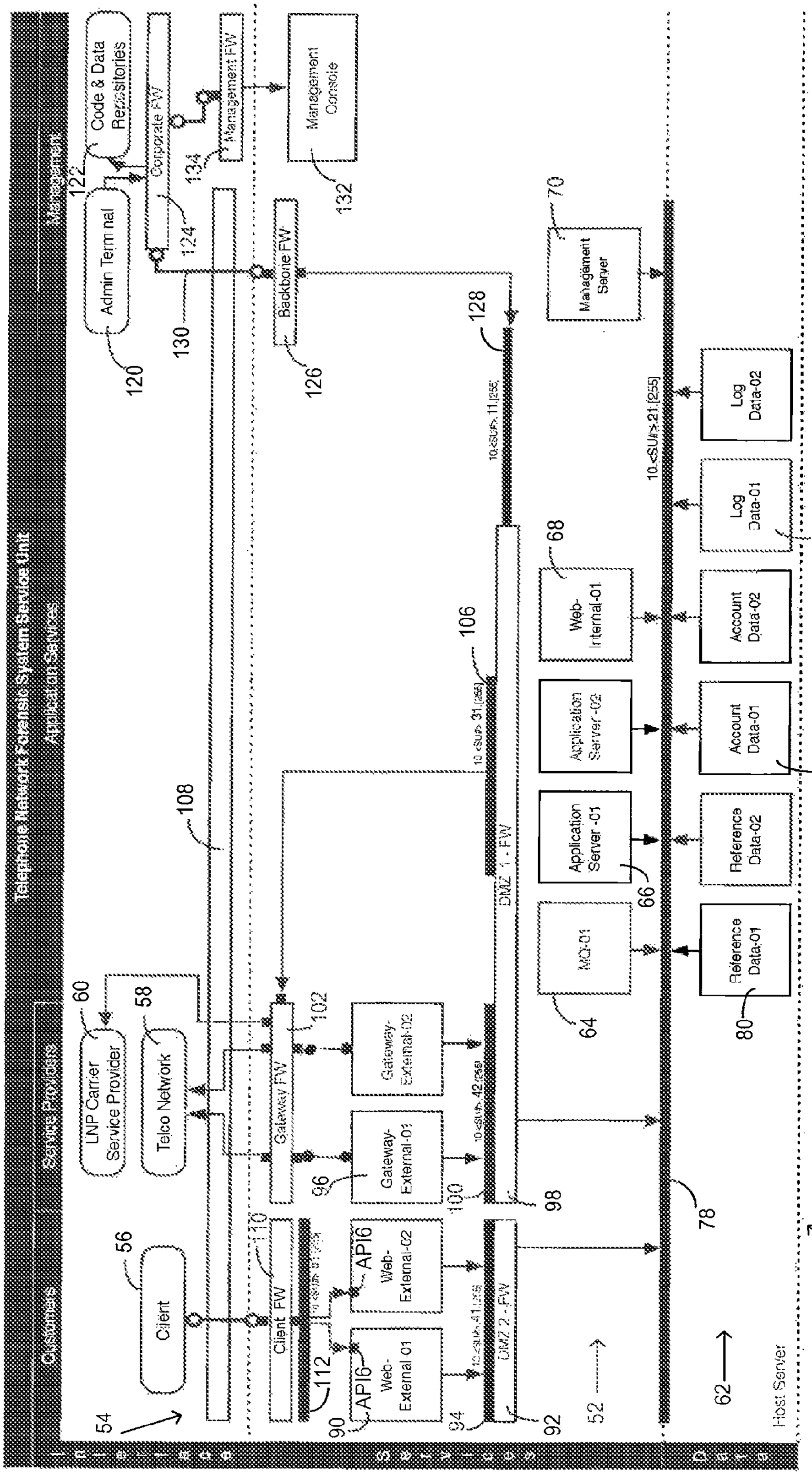

Telephone Network Forensic System Service Unit
Application Services
Management
Service Providers
Customers
Premise
Services
Data
Code & Data Repositories
Admin Terminal
Corporate FW
Management FW
Management Console
Backbone FW
Management Server
LNP Carrier Service Provider
Telco Network
Client
Client FW
Gateway FW
Gateway-External-01
Gateway-External-02
API6
Web-External-01
API6
Web-External-02
DMZ 2 - FW
DMZ 1 - FW
10.<SU#>.41.[255]
10.<SU#>.42.[255]
10.<SU#>.31.[255]
10.<SU#>.11.[255]
10.<SU#>.21.[255]
MQ-01
Application Server-01
Application Server-02
Web-Internal-01
Reference Data-01
Reference Data-02
Account Data-01
Account Data-02
Log Data-01
Log Data-02
Host Server
50
52
54
56
58
60
62
64
66
68
70
78
80
82
84
90
92
94
96
98
100
102
106
108
110
112
120
122
124
126
128
130
132
134

FIG. 2

METHOD OF AND SYSTEM FOR DISCOVERING AND REPORTING TRUSTWORTHINESS AND CREDIBILITY OF CALLING PARTY NUMBER INFORMATION

RELATED APPLICATION

This application claims benefit of U.S. Provisional Patent Application No. 61/179,629, filed May 19, 2009.

COPYRIGHT NOTICE

TECHNICAL FIELD

This disclosure relates to calls placed in telecommunication and information service networks and, in particular, to establishing, for call recipients, the credibility of incoming calls by discovery of and reporting on the credibility of Automatic Number Identification (ANI) information in-line with the incoming calls in progress.

BACKGROUND INFORMATION

ANI (Automatic Number Identification in North America is the 10-digit billing telephone number of the caller) was made available in 1967 to a business telephone customer for toll free circuits (800 or "Inward-WATS") to inform the business telephone customer who was calling because the called business was paying the toll costs of the incoming call. ANI and Calling Number Identification (Caller ID) were made available as products to residential and small business telephone customers to provide them with the 10-digit telephone number of the calling party, and by the late 1980s in some cases the caller's name. Businesses such as banks, call centers, and government entities such as 911 service centers have relied on ANI information as a factor in identity determination; as an element in location discovery; and for call routing assistance, workflow efficiency, and fraud mitigation.

The ability to falsify ANI has been available for over a decade, but only to sophisticated and mostly regulated telecommunications carriers and very large business Users subscribing to expensive multi-line Primary Rate Interface (PRI) telephone circuits. ANI control has a legitimate use. As an example, a large business uses ANI control to display its main telephone number on all outgoing calls from its multiple lines.

The ability to falsify ANI stems from interaction of new technologies with legacy telecommunications architecture. Before the advent of information services network (e.g., Internet) telephony and deregulation, the telecommunications network was a closed system with one or both of a limited number of trusted FCC- and Public Utility Commission-licensed telecommunications companies adhering to a finite set of standards. Telecommunications decentralization and deregulation, as well as Internet telephony (Voice over Internet Protocol (VoIP) technology), have exposed this legacy architecture to an abundance of new telephony products and services that inject calls and calling data from outside the control of the legacy telecommunications network. The

telephony network then delivers to its destinations these calls and associated information, in most cases, without checking their validity. Consequently, this system supplies an opening for criminals to easily place calls with fabricated or "spoofed" ANIs for nefarious purposes. ANI fabrication or spoofing is a low cost, powerful penetration tool used to impersonate identity and location. Multiple companies and, more importantly, technologies exist for the sole purpose of enabling anyone, anywhere, to spoof ANI and Caller ID for pennies each call.

Throughout the past 25 years, telecommunication Users have relied on ANI and have built vital business processes around the incoming calling party telephone number. In addition, most businesses have developed sophisticated inbound telephone answering systems (known as IVR) that answer calls and are programmed with rules-based decision parameters grounded on the ANI. Now, relying on non-validated ANI undermines these critical marketing, technical, and security processes used for authentication, identity, location, and activation in today's financial services, general business, and government enterprises. As one specific industry example, major financial institutions now have compromised critical operations that were built upon the trustworthiness of ANI. Applications such as bank-card activation, credit issuance, money transfers, new account applications, and customer service have all relied on the layer of security ANI has provided. Decisions made using the current non-validated ANI place an enterprise at risk of diminished revenue by limiting new product offerings and increased losses from fraud. Attempted fraud exceeds $50 billion each year in the U.S. alone. Identity fraud is the key driver in these losses. Today, more bank card activation fraud occurs by telephone than by other remote banking channels combined (i.e., not face-to-face), such as ATM, e-mail, and world wide web.

There are several ways in which a motivated individual can take advantage of the current state of the art to manipulate ANI. VoiceXML applications let Users change ANI and Caller ID. An open source PBX software application, such as Asterisk, allows users to manipulate ANI. Competitive service providers and telecommunication carriers can set their own ANI. Moreover, certain companies exist today for the sole purpose of allowing ANI and Caller ID to be spoofed and falsified. Businesses such as Camophone, Telespoof, Covert-Call, and dozens of others offer widely available ANI and Caller ID spoofing for pennies each call.

The consequences of prevalent, facile manipulation of ANI provide motivation to restore integrity to the use of ANI. One major consequence is financial fraud, which is on the rise and is driven primarily by identity fraud. Traditional financial services customer verification tools such as information-based authentication are being compromised. Most financial service companies use ANI as the apex identifier in their telephonic decision-making. If false trust is placed in spoofed ANI, downstream decisions are compromised. Decisions made using current non-validated ANI is placing companies at risk, limiting new product offerings, and increasing losses from fraud. The disclosed approach restores the value of ANI by reestablishing the security of telephone transactions.

There are more financial transactions conducted over the telephone than are conducted on the world wide web, even in today's Internet pervasive environment. Of the more than two billion telephone calls placed annually to U.S. financial institutions alone, nearly all rely on ANI for security, location information, call routing, and identity authentication. Knowing the caller's location or that the caller is in possession of an actual telephonic device is the foundation and an important factor for trusted telephone commerce.

A major nonfinancial consequence is criminal mischief. A Washington state man was sentenced to 30 months in prison, after using ANI spoofing to send SWAT teams to the houses of a dozen innocent, unknowing individuals.

The following is a chronological summary of the evaluation of ANI spoofing and legislative attempts to combat it.

In 2003, VoiceXML applications let Users change ANI, and, at the same time, VoIP telephony entered the marketplace. An open source PBX software application, called Asterisk, allows users to manipulate calling party number information. Asterisk is a software implementation of a telephone private branch exchange (PBX) originally created in 1999 by Mark Spencer of Digium. As an example, if the ANI field is left blank by the Asterisk or carrier switch, any user can easily manipulate the Caller ID information using Asterisk, thereby populating the ANI field with the same misinformation as the spoofed Caller ID. Asterisk allows Users to send spoofed ANI in the same way that businesses had been setting their ANI with PRI lines.

In 2004, a new ANI spoofing service, named Star38, (using VoIP and Asterisk) was launched and gained attention from worldwide mainstream media after USA Today published in its daily paper a front-page article about the service. The same year, others followed such as Camophone, Telespoof, and CovertCall. Over the next year, a dozen additional services started delivering ANI spoofing services.

By 2006, the FCC began investigations into these services, and the House of Representatives and the Senate considered several bills attempting to outlaw use of ANI spoofing for fraudulent purposes. ANI spoofing gained the attention of the mainstream media as SpoofCard announced the cancellation of an account belonging to Paris Hilton that was used to break into the voicemail of Lindsay Lohan to harass her.

On Jun. 27, 2007, the United States Senate Committee on Commerce, Science and Transportation approved and submitted to the Senate calendar Senate Bill S.704, which would have made spoofing ANI a crime. Titled the "Truth in Caller ID Act of 2007," the bill would have outlawed causing "any caller identification service to transmit misleading or inaccurate caller identification information" via "any telecommunications service or IP-enabled voice service." Law enforcement would have been exempted from the rule. A similar bill, HR251, was recently introduced and passed in the House of Representatives. It had been referred to the same Senate committee that approved S.704. The bill never became law because the full Senate never voted on it; it was added to the Senate Legislative Calendar under General Orders, but no vote was taken, and the bill expired at the end of the 110th Congress. On Jan. 7, 2009, Senator Bill Nelson (FL) and three co-sponsors reintroduced the bill as S.30, the Truth in Caller ID Act of 2009, which was the bill referred to the same committee in the Senate. The House of Representatives passed the Truth in Caller ID Act of 2010 in April 2010, but the bill has yet to be reconciled with the Senate version. The new bill states that Caller ID may not be spoofed to be intentionally misleading or inaccurate. No federal bill has yet to be signed into law. Several of the States have passed bills making misleading Caller ID spoofing illegal.

What is needed is a method to detect or report the accuracy and truthfulness of ANI.

SUMMARY OF THE DISCLOSURE

A method of and system for discovering and reporting the trustworthiness and credibility of calling party number information, such as Automatic Number Identification (ANI) or Calling Number Identification (Caller ID) information, or for

inbound telephone calls entails use of real time telephone network status and forensics, network data, locally stored data, and predictive analytics. Practice of the disclosed method is neither detectable by nor intrusive to a calling party, and the method can be implemented into existing enterprise, information services, and telecommunications infrastructures.

The disclosed method performs ANI analysis with the calling party's telephone or telephonic device in a transitional state between an actual or a virtual on-hook condition and an answered condition, and is implemented as follows in a preferred system. When the first indication of an incoming call is detected by a User itself or equipment implementing an Application Programming Interface to communicate with the System, the ANI, along with other information such as the dialed number (DNIS) and incoming trunk identification information, is transferred to the System, using an Applications Programming Interface (API). The disclosed System quickly begins decomposing the calling party number (i.e., supposed telephone or billing number) to check the calling party number validity, check call velocity, compare the originating switch identifier with the NPA-NXX of the calling party number, and check other call number attributes. Calling party number validity relates to format issues for the North America Numbering Plan, such as, for example, whether the area code starts with an impermissible digit ("1" or "0") or whether the calling party number contains greater or fewer than 10 digits. Calling velocity relates to whether an excessive number of calls have been placed by a calling party to one or more Users within a specified unit time period. The NPA-NXX of a calling party number relates to the breakdown of 10-digit number, in which NPA refers to the three-digit numbering plan area (area code) and NXX refers to the three-digit central office (exchange) code.

If a specified one or number of such attributes suggest an anomalous or suspicious calling party number, the disclosed System determines noncompliance of the calling party number, and the System can terminate the procedure and indicate to the User that a calling party number is of low credibility. To continue the analysis of the calling party number, the disclosed System begins to discover the origins of the calling party number, such as telecommunications carrier, line type (e.g., business, government, residence), geo-location, network conditions, and network condition call progress message patterns. The System next begins to probe the calling party number by examining network signaling including call forward messages to ensure probing of the received calling party number and using the telecommunications network by calling and signaling to detect and record status, messages, line conditions (e.g., busy signal), hook switch status, answer and message timings, call forward actions and responses. The origins of the calling party number and the calling number network responses are used to create a real time pattern of all the above elements. The signaling and condition patterns represent, therefore, characteristic "thumbprint" patterns of the calling number telephone network and its call progress functions. The real time pattern is then compared against a historical database of expected call patterns of valid and invalid ANI decomposing processes. Based on the closeness of patterns and the degree of match, a confidence metric is calculated using statistical probabilities. The confidence metric is used by one or both of the User and the System to determine the validity of the ANI. Once the ANI is validated, the recipient can have a higher degree of confidence in the validity of the calling party number and place more trust in it.

The following presents examples of uses, and systems that would benefit from implementation, of the disclosed method.

In the banking industry sector, credit, debit, ATM, and gift cards are mailed to customers. When these cards are received by the recipient, most banks request that the recipient confirm receipt of the card by "activation" of the card. The most preferred method of activation entails placement of a call by a card recipient from his or her home telephone to a toll-free (800) number of the bank to activate the newly received card. The use of a toll-free (800) service by the bank ensures the transmission of ANI information to the bank, even if the consumer has a feature on his or her telephone line to "block Caller ID transmission." The transmitted ANI information is one factor used by the banks to prove that the card in fact is in the intended recipient's possession.

Banks can also use additional factors of authentication to further identify and locate the caller by one or both of asking for personally identifiable information (PII) and relying on voice biometrics, primarily as a consequence of the now unsecured and "spoof-able" nature of ANI. PII may be, for example, a social security number or date of birth. Using PII to conduct information-based authentication has its challenges and risks. Information based authentication using PII such as social security numbers or a mother's maiden names exposes the bank to additional risk. PII information is regulated, and, if the PII information in the bank's possession is lost or stolen from the bank, large costs and fines can be levied against the bank by government entities enforcing current data breach laws. Moreover, because of the high number of past data breaches, a very high percentage of consumers have had their PII data compromised already, making PII available to criminals for use in ID theft. (In 2009, the Identity Theft Resource Center reported 493 breaches and 300 million records exposed.) In addition, another aspect of PII access has further eroded the value of information-based authentication. Social networking websites such as FaceBook, LinkedIn, MySpace, Ancestry, Twitter, and dozens more all contain and share PII with the public, further de-valuing the use of PII knowledge as a tool for identity authentication. ANI is one of the authentication tools available to banks that are not PII based for telephone-based transactions. The disclosed method helps restore the value lost to spoofing and fraudulent ANI transmissions, providing a powerful new tool to banks to authenticate their customers by again using and trusting validated ANI as a factor in authentication for the telephone channel.

The disclosed method and system return the trust, credibility, and security to incoming telephone calls by discovering and reporting on inaccurate ANI information in-line with a call in progress, allowing trust to be correctly placed in real time that the ANI information has not been altered or set incorrectly or "spoofed" by the caller or a telecommunications carrier. The disclosed system and method can be used by business, government, and consumers alike, as well as provide an existing telecommunications carrier a tool to improve the security and value of its network.

Additional aspects and advantages will be apparent from the following detailed description of preferred embodiments, which proceeds with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a hybrid system process block and method step flow diagram of the disclosed method of and system for determining trustworthiness and credibility of calling number information relating to calls placed in a telecommunications network.

FIG. **2** is a block diagram of a telephone network forensic system service unit suitably configured to implement preferred methods of determining credibility of calling party number information performed in accordance with the hybrid process block and method step flow diagram of FIG. **1**.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In telephony, the calling party number information is delivered and described in many different ways. This document uses the acronym "ANI" to describe the following types of calling party number information systems and descriptions, unless any one of the following terms needs to be used specifically to communicate clearly: Caller ID or CID; Calling Party Number or CPN; Calling Number Identification (Identifier) or CNID; Calling Party Identification (Identifier) or CPI; Automatic Number identification (Identifier) or ANI; Automatic Number Identification Information Digits or ANI II, ANI 2, II digits; Billing (Billed) Number or BN; Caller (Calling) Line Identification or CLID; A-Number; and Calling Party or CP. The term "call" is used in this document to define any connection over a telecommunications or an information service network and includes, but is not limited to, landline, wireless, modem, facsimile, Session Initiation Protocol (SIP), and Voice over Internet Protocol (VoIP) transmissions.

The Problem the Disclosed Method and System Solve

With the deregulation and de-centralization of the telecommunications landscape and the introduction, proliferation, connection, and integration of information service network telephony (e.g., Internet VoIP) into the Public Switched Telephone Network (PSTN), combined with the ability to control the transmission of a caller's telephone number to a called party in the many forms (most commonly called ANI and Caller ID), is now controllable by the calling general public.

Before the dramatic marketplace changes outlined in this section, a calling party's number was securely transmitted by a regulated telecommunications company to the called party.

This newly found control of the telephone network by the public at large, mainly through use of VoIP connections, has caused the recipient of a telephone call to distrust in the accuracy and truthfulness of a calling party's telephone number.

The following description of implementations of preferred embodiments is presented with reference to FIG. **1**, which is a hybrid system process block and method step flow diagram. The diagram includes User related function blocks and system related process module blocks, as indicated in FIG. **1**.

An Incoming Call **2** block represents an event in which a called party (User) receives a telephone call delivered by a telecommunications carrier from a calling party. The carrier delivers an ANI, (usually 10 digits long in North America) along with or before the voice portion of that call is connected to the called party.

A Transmission **4** block represents a User (such as a bankcard activation center or a 911 emergency services call center) transmitting the ANI to the System before the call is answered and while the calling party hears one or more ringing tones. This transmission before the call is answered (goes off-hook) by the User enables the calling party's telephone to be in a more predictable and detectable transitional state. This transmission step may be performed through any conventional data transmitting technique, such as over the Internet with a virtual private network connection, a remote or private circuit connection, or a local area network using any data transmission model such as HTTPS, SOAP, or XML. This transmission step is not limited to offering only ANI information. For example, the User may transmit the time of day, trunk number, ANI II digits, dialed number information (DNIS), SIP header and routing information, transaction number, unique identifier, or other information or data that may be helpful to the System, or to the User if re-transmitted back to the User, for example, to assist in re-associating a transmission with the calling party's call.

An Application Programming Interface (API) **6** block represents the User of the System receiving the data and information described with reference to Transmission **4**, and then re-transmitting the data in a standardized format to the System. The System sends, to the User, data and information in a standard format that are described in a Determine **20** block of the System. API **6** could make format standardization of data in any known manner, including fixed field database structure, name/value pairs, XML, tab delimited, comma delimited, fixed width, or variable length. API **6** could make the subsequent transmission in any known manner, providing an electronic data connection to an active database or data management system such as Oracle or a proprietary or open source software program. The machine or computer may record the data on any known information storage device, including RAM, magnetic media (e.g., a hard disk drive), or any other electronic medium.

A Calling Party Compliance block **7** represents decomposition of the calling party number to check its validity, check call velocity, compare the originating switch identifier with the NPA-NXX of the calling party number, and check other call attributes. If it determines noncompliance of the calling party number, the System can terminate the procedure and indicate to the User that a calling party number is of low credibility. Otherwise, System operation proceeds as described below.

A Carrier Discovery **8** block represents a query of available network-accessible Local Number Portability (LNP) databases, such as the ones maintained by North American Numbering Plan Administration (NANPA), NetNumber, or TNS, to determine the current telecommunication carrier that services and owns the ANI number delivered in Transmission **4** from the incoming call placed to the called party in Incoming Call **2**. This query could be performed via the Internet using a secure TCP/IP protocol or other methods, such as Signaling System 7 (SS7), ATM, ITU-T, SIGTRAN, or Enum. In another variation, a locally stored database could be queried to determine the current telecommunication carrier that provisioned the line of the ANI from the incoming call placed to the called party in Incoming Call **2**.

A Line Type **10** block represents use of databases of telephone circuit types (such as, for example, business, wireless, residential, pay telephone, prison telephone, VoIP, satellite, pre-paid, post-paid, SIP, or pager) and information from other process modules or steps in the System such as Carrier Discovery **8** to assign a Line Type **10** to the ANI from Incoming Call **2**. A Line Type **10** database is created by assigning, analyzing, and building a compiled database of ANI Line Types from commercially available database(s) such as Targusinfo, InfoUSA, Acxiom, or others with databases maintained by telecommunication carriers or third party providers, such as Verizon, TNS, or NANDA, and from proprietary databases developed from primary research or housed on behalf of clients (numbers on which fraud has been previously committed or numbers assigned by the client as high risk). The compilation is performed by analysis of source quality metrics or other known techniques. These databases could be network (Internet, SS7) accessible or locally stored in the System or by combination. In another embodiment, Line Type **10** would be determined from a carriers business practices. Such an example would be Integra Telecommunications, which, at the time of this writing, provides only business line types.

Geo-location **12** block represents determination of the city and state, latitude, longitude, and other geospatial information about the ANI. The geo-location is determined by querying one or more databases, such as Telcordia, that provide routing guides using available rate center data providing geospatial data inferred from an ANI. International numbers can also be identified, using country-calling codes. Use of attribute data and vector data models collected, compiled, and analyzed for specific areas such as LATAs (Local Access Transport Areas) or a carriers switch serving areas enables inference of discrete locations from the analysis of data contained in the attributes associated with each ANI.

In an alternative embodiment, the determination of the caller's location can also be made by use of the Home Location Register (HLR) or other carrier-based real time database to determine which switch or end office or what wireless telephone offices are managing the call, and then to calculate the location of that switch. In a second alternative embodiment, a third party geospatial technology or vendor such as Geografx can be used to provide the geo-location of the caller. In a third alternative embodiment, the determination of the callers location can also be made utilizing IP address information where available. Standards such as IPv6 define routable home IP address information that can be used to determine geo-location information. Geo-location may be returned as Geo-location **12** data that are used to determine the serving switch to assist in call pattern recognition and creation represented by a Storage **16** block, a Real-Time Pattern **17** block, a Compare **18** block, an Expected Patterns **19** block, and Determine **20** block.

A Network Condition **14** block represents placement by the System of one or more outbound calls to the telephone number represented by the received ANI in Incoming Call **2** before the incoming call to the User is answered, which is represented by a Call Answer **26** block. This enables the calling telephone line to be in a predictable and detectable state because call waiting and other features are unavailable at this time on most line types during this unanswered off-hook ringing state. These calls should be placed from a switch that uses SS7 services or with a VoIP service allowing for SIP and/or SIP-T messaging or other available network connection types to allow for the maximum amount of call progress messaging and maximum number of details to be recorded such as call forwarding and route information and status. Network condition, line-status, call progress information, and call progress messages and their associated timing information are collected in Network Condition **14**. The outbound call(s) query the current network condition of the telephone number (such as, for example, busy, ring then answer, call forward then answer, and ringing no answer). Such calls produce a series of conditions, each with a status and response with specific timing associated with each call progress message or network state.

In addition to network messages, available audio energy detection and determination methods are used, and the results are analyzed with the use of dedicated or shared digital signal processing (DSP) hardware and/or software to determine the type of answer condition and line type (such as a answering machine, fax machine, carrier-based voicemail, business line, automated attendant, or call progress tones including intercept tones, reorder tones, or guard tones). These status, conditions, and responses are categorized with associations and timings for later analysis performed in Determine **20**. In another variation, data connections (such as SS7 or virtual private network) to telecommunications providers may provide additional information as to the network condition of the ANI received in API **6**.

Connections to the telecommunications or third party provider may use new methods (such as real-time call detail record (CDR) analysis), existing methods (such as a CALEA interface or home location registers (HLR)), or billing ports and computer telephony interface (CTI) ports to access line status information. An example of the type of query and response in this variation would be to query a carrier through currently available means, such as a VPN, dedicated circuit, or SS7 connection, to determine whether a specific ANI is currently in a ringing state with the dialed number (DNIS) transmitted to the System in Transmission **4**. In another embodiment, the can status returned to the System from such query could be "in-progress" (answered) if the ANI was transmitted to the System in Transmission **4** after the call had been answered. In another embodiment, after the User receives the call in Incoming Call **2**, and after completion of Call Answer **26**, the User is informed that the System or another system managed by the User will be calling back the calling party while looking at real time network forwarding messages and other signaling after the current call terminates. This is done to verify that the received ANI transmitted in Incoming Call **2** is reachable by an outbound call and is, in fact, the number the User is using to place the call received in Incoming Call **2**. A new outbound call is then placed to the ANI in incoming Call **2** to the calling party to verify that the calling party is in fact reachable at the number that was received in Incoming Call **2**. This outbound call is placed from a switch that uses SS7 services or with a VoIP service allowing for SIP-T messaging or other available network connection types. Such placement of the outbound call allows for the maximum amount of call progress messaging and number of details to be used by the System, so as to detect whether a call forward or other message is detected after the call is placed to the User, thus indicating the call was potentially not connected to the ANI from Incoming Call **2**.

Storage **16** represents sorting by network codes, condition, and timing the responses received from the outbound call(s) for storage and later analysis for validity, pattern recognition, and other risk factors by such elements as network condition, time of day, call progress messages, response times by carrier, variability in status messages, latency in telecommunications networks, and statistical probabilities. The analyzed responses are then sorted and formatted with all other data obtained in API **6**, Carrier Discovery **8**, Line Type **10**, Geo-location block **12**, and Network Condition **14** as patterns in a database represented by Real Time Patterns **17**.

In Real-Time Patterns database **17**, all the data from Storage **16** that were persisted as patterns are stored as a database for analysis, represented by Compare **18**. The following is an example of a valid ANI call pattern: a call placed to a Verizon (potentially Frontier) residential landline number that is in a previous GTE area in Oregon, does not have carrier-based voicemail activated as an optional feature, and is in an outbound ringing state will show as busy, while the same line that has carrier-based voicemail and call waiting features active on that line will show 1) a partial ring back message and then 2) an answer from the voicemail system within three seconds. In addition, the voice energy analysis and determination from the digital signal processing (DSP) would indicate that an answering device answered the call. In an invalid ANI call pattern, if it is determined that a human being answered, as taught by one or more complete ring cycles (six or more seconds after call is placed, with no call transfer message) along with a digital signal processor DSP determination of "human" answer, or if a ring without an answer pattern occurs, then the calling party in Incoming Call **2** would not have been calling the User in Incoming Call **2** because the call waiting feature is disabled on this line type in an outbound ringing transitional state.

In Compare **18**, the pattern data stored in the Real-Time Patterns database **17** from Storage **16** are then compared against expected pattern results found in an Expected Patterns database **19**. One or more patterns will be retrieved from Expected Patterns **19** based on information from Carrier Discovery **8**, Line Type **10**, and Geo-location **12**. Patterns need not be exact to match between Expected Patterns database **19** and Real-Time Patterns database **17**. Matching logic indicating the closest comparable candidate between the Expected Patterns database **19** and the Real-Time Patterns database **17** is chosen as an input to the statistical probability calculation. The pattern recognition can take into account any statistical reference tables. For example, if a call is in an outbound ringing state, there is a high degree of probability that the calling party is in fact calling the User.

The Expected Patterns database **19** is composed of, but not limited to, baseline repeatable call flow patterns that are built in advance utilizing run-time, call statistics, hour usage and traffic patterns, and call frequency tables. The Expected Patterns **19** baseline database is created through empirical testing and sampling of known conditions in an advance of run-time process including placing multiple calls to a series of telephone numbers representative of the call handling process of each of the carriers throughout their network. The data include all SS7, VoIP, or wireless network messages, including their ordering and timing between messages. In addition, the Expected Patterns **19** data call patterns may be defined and recorded for each switch type and location within a carrier's network for valid ANI scenarios, then invalid ANI scenarios. The call patterns may include every message received from the network with their associated time and duration facts while placing a call, as well as messages received from the digital signal processing (DSP) monitoring and analysis during the call with associated time and duration facts, first for a valid ANI pattern call, then for an invalid ANI pattern call. These patterns are built, tested, and persisted for each unique combination of carrier (Carrier Discovery **8**) and line type (Line Type **10**), and optionally of geo-location (Geo-location **12**), as defined, for example, by serving switch. In addition to these elements, metadata are added to the call pattern data with elements such as time of day, frequency of recurrence, and statistical likelihood of call.

The Expected Patterns database **19** can be updated with each new ANI analysis while in run-time production, thereby creating a continuously learning system that provides ever-widening coverage of patterns. As part of the learning system, information stored in Storage **16** can be mined for additional information regarding new carrier information, new status, and new combinations of status messages and timing to be used to improve and enrich the Expected Patterns database **19**. This creates a learning system that benefits all steps, especially Determine **20**. The Expected Patterns database **19** will evolve through continued use of the System, adapting to telecommunications advances and creating a learning Expected Patterns database **19** with continuous feedback and updating.

In Determine **20**, the results from Compare **18** are analyzed for normalcy deviation and statistical match to patterns and their timing or duration between messages or conditions. This analysis entails comparing the real time patterns to previously expected call patterns of valid and invalid calling party decomposing processes to make a degree of match interpretation. In turn, these and other attributes or elements may be used to generate a score or metric of the validity of an ANI or, alternatively, as a singular determination such as "valid" or "invalid" or as a tiered system such as "red," "yellow," "green." Each additional attribute or element such as carrier, line type, geo-location, time of day, match of real time pattern to expected pattern is assigned a weighted value as factors of a confidence metric. A confidence metric is produced using statistical methods to indicate the probability that the ANI is correct. The metric can be adjusted by application or by recipient, based on previously defined thresholds. For example, a bank may consider a VoIP telephone to be of significantly higher risk, whereas a voicemail application requiring verification may consider a VoIP telephone to be of no more significant risk than a landline or wireless. Determine **20** then sends the metric along with other optional data as outlined in Transmission **4**, such as the time of day, trunk number, ANI II digits, dialed number information (DNIS), transaction number, or other information or data that may be helpful to the User, such as assisting in re-associating this transmission with calling party's call, is sent back to API **6**.

In another embodiment, analysis of call detail and other records by telephone number may also create new variables, including velocity of calls measured and metrics, to determine whether a telephone number or set of telephone numbers has been dialed excessively by an ANI, which could be one indication of a fraud pattern. The velocity measure over a period could be set by an application. As an example, more than 15 call requests in a 15-minute period may indicate a brute force attack and could be consider higher risk. This attribute would be an element used in the scoring and metric of accuracy and security of an ANI. In another embodiment, the System may gather additional information that may be useful to the User from additional systems, vendors, processes, or metadata from one or more of the steps taught in this application, such as caller name, address, city, state, zip code, latitude/longitude, equipment type, caller location, IP address, or other information, in addition to predictive scores or metrics such as a fraud score, risk score, credit score, marketing score, affinity score, expansion score, or warning indicators for bankruptcy, deceased, or information from a consortium database such as calling velocity to multiple locations within a specified time period, or known frauds, and then passed to API **6** along with the ANI validity metric.

A Metric Received **22** block represents receipt from API **6** of a confidence metric developed, scored, and created in Determine **20**, indicating the probability that the ANI from Incoming Call **2** is valid. API **6** sends such information to Metric Received **22** during the call (either pre-answer or post-answer) or at a later time (e.g., daily, weekly, or monthly), either individually or in aggregate in a batch data duration. Other data potentially received include optional data as outlined in Transmission **4**, such as the time of day, trunk number, ANI II digits, dialed number information (DNIS), transaction number or other information or data that may be helpful to the System or the User such as assisting in re-associating this transmission with calling party's call.

Processed **24**A and **24**B blocks represent alternative processing of the metric and other information taught in Metric Received **22**. The information delivered to and processed by Processed **24**A is analyzed, scored, and acted upon in real time. This processing is performed according to a set of rules and processes by the User or by a third party rules engine such as ALI or any other commercially available system or any proprietary system that routes or makes decisions on the handling of any call, caller or call flow, in accordance with the

recipient's algorithm, to the proper queue or IVR or agent, along with other fraud or call processing rules or procedures. The User's telephonic business rules engine may provide additional call scripting based on one or both of the metric and the additional information provided from the System or the Users business rules. The information delivered to and processed by Processed **24**B is analyzed, scored, and acted upon as a batch process at, for example, the close of a business day. The processing is performed according to a set of rules and processes by the User or by a third party rules engine, as described above for Processed **24**A.

A Call Answer block **26** represents answering by User of the call by an off hook or supervision signal or by data packet sent to the Users' providing telecommunications carrier. The call is then processed.

Relationship, Flow and Logic Between the Steps, Methods and Elements

The preferred relationship among elements, including preferred logic and chronological order, is shown in FIG. **1**. The System performs ANI analysis to determine credibility of calling party information as the calling party's telephone or telephonic device is in a transitional state between an actual or a virtual on-hook condition and an answered condition. The System process preferably begins at Transmission **4** and ends at API **6**. As shown in the diagram, Transmission **4** preferably occurs before API **6**, which preferably occurs before Carrier Discovery **8**, and so forth. However, the order of many of these steps may be changed. By way of example but not limitation, Line Type **10** may occur during or before Carrier Discovery **8**, or during, or before Geo-location **12**. Moreover, Network Condition **14** could occur during or before either or both of Carrier Discovery **8** and Line Type **10**, as long as sufficient time remained to make the proper decision at Determine **20** before Call Answer **26**.

In another embodiment, Carrier Discovery **8**, Line Type **10**, Geo-location **12**, further, even Network Condition **14** could be altered or adjusted so that, if the data received in Line Type **10** were "prison telephone" or "pay-telephone," Carrier Discovery **8**, Geo-locate **12**, Network Condition **14** could be skipped or Geo-locate **12** could be preformed to verify the accuracy of data at Line Type **10** before moving to Network Condition **14** through Metric Received **22**.

In another embodiment, the System may be implemented using software running on a local machine at the location of the User and incorporated into its own processes could use the disclosed method taught here to achieve the same trustworthiness and validity metric. This System can be envisioned as a hosted solution, with software installed on client's computer system having associated databases and network connections, or alternatively, as a hardware appliance, prepackaged server, or system including the System and necessary equipment to function installed on client premises. The solution may be a combination of the above-mentioned deployment options.

FIG. **2** is a block diagram illustrating a preferred telephone network forensic System **50** that uses telecommunication links to establish information request and data information communication paths among a User, a telecommunications network, and external data sources to determine credibility of calling party number information of an incoming call to the User. System **50** is configured with a services layer **52** that provides core application services in the credibility analysis of ANI of a call placed to a User. Services layer **52** is linked to an interface layer **54** to receive messages from a Client or User **56** requesting ANI processing and to communicate with a telecommunications network **58** to access call information data or place a test call to the supposed calling party number and an LNP carrier service provider **60** to access call information data. (Process blocks **2**, **4**, **22**, **24**A, **24**B, and **26** shown in FIG. **1** relate to actions performed by or presented to User **56**.) Services layer **52** is also linked to a data layer **62** for access to internally stored call information data used to analyze ANI.

Services layer **52** includes a message queue server **64** and an application server **66** that process incoming call ANI verification requests. Message queue server **64** receives incoming ANI and delivers the results obtained by operation of application server **66**. Message queue server **64** supports the infrastructure for scalability and operational flow of System **50**. Application system server **66** fulfills a call verification request directed by message queue server **64** by controlling and coordinating the ANI processing steps performed as outlined in FIG. **1**. Message queue server **64** has an address to which all other servers provided in System **50** can direct requests for various processing tasks. Thus, the other servers in System **50** request information or deliver data through message queue server **64**, which routes data and queries for processing by the appropriate system servers. This message queue server **64** centric architecture permits expansion of System **50** without disruption of operations of other system servers. A web internal server **68** runs queries through services layer **52** to perform internal test applications and emulate system performance without access to or by systems external to System **50**. A management server **70** performs an administrative function of monitoring the overall system operational status (e.g., checking for faults in ANI processing) of servers in services layer **52** and data layer **62**.

Services layer **52** is linked through a virtual switch **78** to data layer **62**, which includes a reference data server **80** that contains a carrier database of internal information about operational and organizational characteristics for commercially accessible telecommunication carriers, valid NPA-NXX codes, valid NPA-NXX codes as to geo-location, line type, and other information characterizing proper ANI. (Process blocks **7**, **10**, and **12** shown in FIG. **1** relate to cooperative actions performed by application server **66** and reference data server **80**.) An account data server **82** contains User account configuration information, and a log data server **84** tracks all transactions performed by System **50** for billing services, analysis, troubleshooting, and call progress message pattern updates. (Process blocks **16**, **17**, **18**, and **19** shown in FIG. **1** relate to cooperative actions performed by application server **66**, reference data server **80**, and account data server **82**.)

Services layer **52** and interface layer **54** are linked by multiple communication paths. Specifically, services layer **52** is linked to a web external server **90** through a firewall **92** and virtual switch **94**, to a gateway external server **96** through a firewall **98** and virtual switch **100**, and to a gateway firewall **102** through firewall **98** and virtual switch **106**. These firewall-virtual switch combinations provide secure interface within services layer **52** and from interface layer **54** to services layer **52** and data layer **62**. A User **56** located outside System **50**, as indicated by outside world boundary **108**, accesses System **50** through a client firewall **110** and virtual switch **112** to transmit to web external server **90** ANI associated with an incoming call verification request and to receive from web external server **90** results obtained after system processing of the ANI. The results obtained include a calculated confidence metric representing the credibility of the calling party number (FIG. **1**, process block **20**). Applications Programming Interface **6** is implemented by web external server **90** and defines a standard format by which communication takes place between web external server **90** and User **56**. Services layer **52** interfaces with telecommunications network **58** (FIG. **1**, process block **14**) through gateway external server **96**, firewall **98** and a virtual switch **100**, and gateway firewall **102** to place a test call to the supposed calling party number of the incoming call to User **56**. Services layer **52** interfaces with LNP carrier service provider **60** (FIG. **1**, process block **8**) to access (sometimes by purchase) call information data and to return accessed data to message queue server **64** through application server **66**, to virtual switch **78** and firewall **98**, through virtual switch **106** and gateway firewall **102**.

An administrative terminal **120** and associated code and data repositories **122** are linked through a corporate firewall **124** at interface layer **54** to System **50** and are routed to services layer **52** through a backbone firewall **126** and virtual switch **128**. This administrative link to System **50** allows corporate level management access, from across outside world boundary **108**, to System **50** via a secure link **130** to, for example, perform demonstrations of system functionality and obtain operational status of System **50**. A management console **132** in services layer **52** links administrative terminal **120** through a management firewall **134** to run the virtualization software of System **50**.

FIG. **2** shows six servers in duplicate to indicate operational, equipment, and virtual appliance redundancy to ensure continuing service in the event of localized failure of any one of the six servers of System **50**.

Basic and Optional Elements of Disclosed Method and System

The System can be implemented with all, part, or limited functionality of any method or step taught in this patent application or any combination. For instance, if User is interested only in validation of the ANI of wireless callers, and the LNP information learned in Carrier Discovery **8** is known to only provision wireless services, the Line Type **10** and possibly method Geo-Location **12** may not be required.

For situations in which the System had direct access to real time line status information by connections to carriers to disclose line status as taught is the first variation in Network Condition **14**, the requirement to perform additional network status queries may not be required.

Another system benefiting from implementation of the disclosed method is telephones used by consumers or individuals at work. Frequently today, consumers and individuals at work are relying on Caller ID information to determine who is calling them. This is increasing important with a relatively new and disturbing trend called Phishing. Phishing is a practice of fraudulently taking on the persona of an institution, such as a bank, for the purpose of defrauding a consumer or an individual at work. As an example, a person receives a telephone call, and his or her Caller ID device displays “Bank of ABC.” The “Bank” has called to verify credit card transactions for the security of the cardholder. The true caller is, however, in Eastern Europe and has no affiliation with Bank of ABC, but has simply used Caller ID spoofing to defraud the call recipient into believing his or her bank has placed the call. If the consumers or individuals at work fall prey to this fraud, the called person may share Personally Identifiable Information (PII) with the fraud perpetrator, allowing the fraud perpetrator to do financial harm by using the newly acquired PII from the victim. The disclosed method helps mitigate this fraudulent and costly practice.

It will be obvious to those having skill in the art that many changes may be made to the details of the above-described embodiments without departing from the underlying principles of the invention. The scope of the present invention should, therefore, be determined only by the following claims.

The invention claimed is:

1. A method of determining a source origin confidence metric of a calling party number or billing number associated with an incoming call to a called party telephonic device from a calling party telephonic device, comprising:

receiving by an electronic system associated with the called party telephonic device the calling party number or billing number, wherein the electronic system receives the calling party number or billing number from the called party telephonic device;

after receiving the calling party number or billing number and before the incoming call is answered, gathering by the electronic system associated with the called party telephonic device operational status information associated with the calling party number or billing number, and

determining by the electronic system associated with the called party telephonic device the source origin confidence metric for the calling party number or billing number.

2. The method of claim **1**, further comprising receiving by the electronic system associated with the called party telephonic device characteristics of the incoming call.

3. The method of claim **2**, wherein characteristics of the incoming call include one or more of time of day, trunk number, ANI II digits, dialed number information, an identifier of an originating switch, SIP Header information, SIP routing information, transaction number, call frequency indicator, SS7 data or a unique call identifier.

4. The method of claim **1**, further comprising determining by the electronic system associated with the called party telephonic device whether the format of the calling party number or billing number is valid.

5. The method of claim **4**, further comprising upon determining that the format of the calling party number or billing number is invalid, generating a message by the system associated with the called party telephonic device that indicates the calling party number or billing number is invalid.

6. The method of claim **1**, further comprising obtaining a number of calls within a given timeframe that have been originated from the calling party number or billing number.

7. The method of claim **6**, further comprising determining by the system associated with the called party telephonic device whether the number of calls within a given timeframe that have been originated from the calling party number or billing number exceeds a threshold.

8. The method of claim **1**, further comprising:

adjusting by the system associated with the called party telephonic device the source origin confidence metric based on personal risk factors of an entity associated with the calling party number or billing number.

9. The method of claim **8**, wherein the personal risk factors include one or more of fraud score, risk score, credit score, marketing score, affinity score, expansion score, or warning indicators for bankruptcy, or whether a person associated with the calling party number or billing number is deceased.

10. The method of claim **8**, further comprising:

retrieving consortium information by the system associated with the called party telephonic device from an external database.

11. The method of claim **10**, wherein the external database includes data for calling velocity to multiple locations within a specified time period for the calling party number or billing number, or known fraudulent calling party numbers or billing numbers.

12. The method of claim **1**, wherein the operational status information associated with the calling party number or billing number includes telephone line status information associated with the calling party number or billing number.

13. A method for authenticating a calling party, comprising:

receiving an incoming call from a telephonic device at a call center telephonic device;

receiving a calling party number or billing number associated with the received incoming call by the call center telephonic device;

prior to answering the incoming call, requesting by the call center telephonic device a source origin confidence metric for the calling party number or billing number from an electronic system associated with the call center telephonic device, wherein the confidence metric is determined based on operational status information of the calling party number or billing number;

receiving by the call center telephonic device the confidence metric for the calling party number or billing number; and

answering the incoming call following receipt of the source origin confidence metric.

14. The method of claim **13**, further comprising:

determining a script for the incoming call based on the received source origin confidence metric.

15. The method of claim **13**, further comprising:

providing an additional call center metric to the electronic system associated with the call center telephonic device, wherein the additional call center metric is used to adjust the source origin confidence metric.

16. The method of claim **13**, wherein the source origin confidence metric is a probability that the calling party number or the billing number is valid.

17. The method of claim **13**, wherein the source origin confidence metric indicates either the calling party number or the billing number is valid or invalid.

18. The method of claim **13**, wherein the source origin confidence metric indicates a calling party number or billing number validity indicator, wherein the validity indicators comprise a static set of predetermined indicators.

19. The method of claim **13**, further comprising:

adjusting by the electronic system associated with the call center telephonic device the source origin confidence metric based on personal risk factors of an entity associated with the calling party number or billing number.

20. The method of claim **13**, wherein the personal risk factors include one or more of fraud score, risk score, credit score, marketing score, affinity score, expansion score, or warning indicators for bankruptcy, or whether a person associated with the calling party number or billing number is deceased.

21. The method of claim **13**, wherein the operational status information of the calling party number or billing number is based on call progress information gathered by placing an outgoing call to the calling party number or billing number and receiving call progress messages associated with the outgoing call.

22. The method of claim **13**, wherein the operational status information associated with the calling party number or billing number includes telephone line status information associated with the calling party number or billing number.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

Page 1 of 1

PATENT NO.	: 9,001,985 B2
APPLICATION NO.	: 13/567592
DATED	: April 7, 2015
INVENTOR(S)	: Cox et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the title page, item 73, please replace “TrustIP, Inc.” with --TrustID, Inc.--.

Signed and Sealed this
Thirteenth Day of October, 2015

Michelle K. Lee

Michelle K. Lee
Director of the United States Patent and Trademark Office

Exhibit 2

US008238532B1

(12) **United States Patent**
Cox et al.

(10) **Patent No.: US 8,238,532 B1**
(45) **Date of Patent: Aug. 7, 2012**

(54) **METHOD OF AND SYSTEM FOR DISCOVERING AND REPORTING TRUSTWORTHINESS AND CREDIBILITY OF CALLING PARTY NUMBER INFORMATION**

(75) Inventors: **Patrick M. Cox**, Newberg, OR (US); **Richard J. Greene**, Portland, OR (US); **Joseph H. Bockelman**, Springboro, OH (US); **Shreyas Saitawdekar**, Portland, OR (US)

(73) Assignee: **TrustID, Inc.**, Portland, OR (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 206 days.

(21) Appl. No.: **12/783,405**

(22) Filed: **May 19, 2010**

Related U.S. Application Data

(60) Provisional application No. 61/179,629, filed on May 19, 2009.

(51) **Int. Cl.**
H04M 15/00 (2006.01)
H04M 17/00 (2006.01)

(52) **U.S. Cl.** **379/114.14**; 379/127.02; 379/144.03

(58) **Field of Classification Search** 379/114.14, 379/121.01, 143.01, 144.03, 127.01, 127.02
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,699,416	A *	12/1997	Atkins	379/115.01
5,963,625	A *	10/1999	Kawecki et al.	379/127.01
6,307,926	B1 *	10/2001	Barton et al.	379/189
6,947,532	B1 *	9/2005	Marchand et al.	379/114.14
7,912,192	B2 *	3/2011	Kealy et al.	379/114.14
2007/0271339	A1 *	11/2007	Katz	709/204

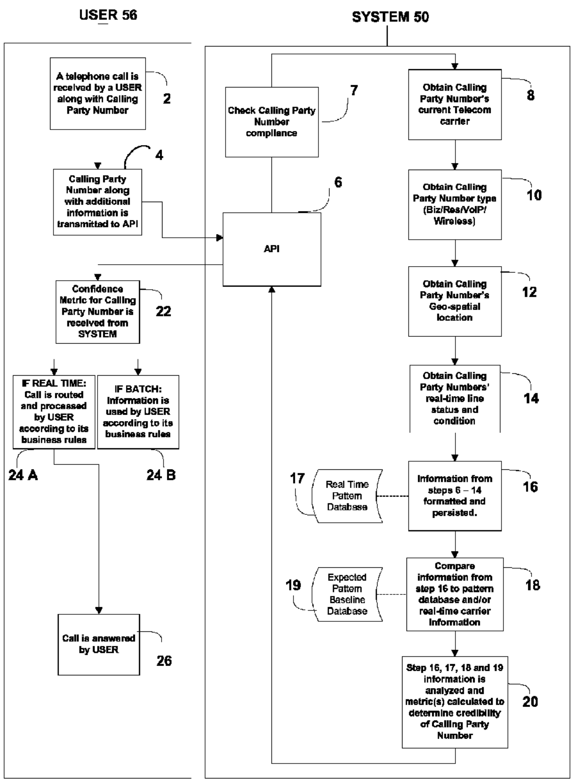
* cited by examiner

Primary Examiner — Binh Tieu
(74) *Attorney, Agent, or Firm* — Sterne, Kessler, Goldstein & Fox p.l.l.c.

(57) **ABSTRACT**

A method of and system for discovering and reporting the trustworthiness and credibility of calling party number information, such as Automatic Number Identification (ANI) or Calling Number Identification (Caller ID) information, or for inbound telephone calls. The disclosed method entails the use of real time telephone network status and signaling, network data, locally stored data, and predictive analytics. Practice of the disclosed method is neither detectable by nor intrusive to the calling party, and the method can be implemented into existing enterprise, telecommunications, and information service infrastructures.

52 Claims, 2 Drawing Sheets


USER 56
SYSTEM 50
A telephone call is received by a USER along with Calling Party Number
2
Calling Party Number along with additional information is transmitted to API
4
Confidence Metric for Calling Party Number is received from SYSTEM
22
IF REAL TIME: Call is routed and processed by USER according to its business rules
IF BATCH: Information is used by USER according to its business rules
24 A
24 B
Call is answered by USER
26
Check Calling Party Number compliance
7
API
6
Obtain Calling Party Number's current Telecom carrier
8
Obtain Calling Party Number type (Biz/Res/VoIP/ Wireless)
10
Obtain Calling Party Number's Geo-spatial location
12
Obtain Calling Party Numbers' real-time line status and condition
14
Real Time Pattern Database
17
Information from steps 6 – 14 formatted and persisted.
16
Expected Pattern Baseline Database
19
Compare information from step 16 to pattern database and/or real-time carrier information
18
Step 16, 17, 18 and 19 information is analyzed and metric(s) calculated to determine credibility of Calling Party Number
20

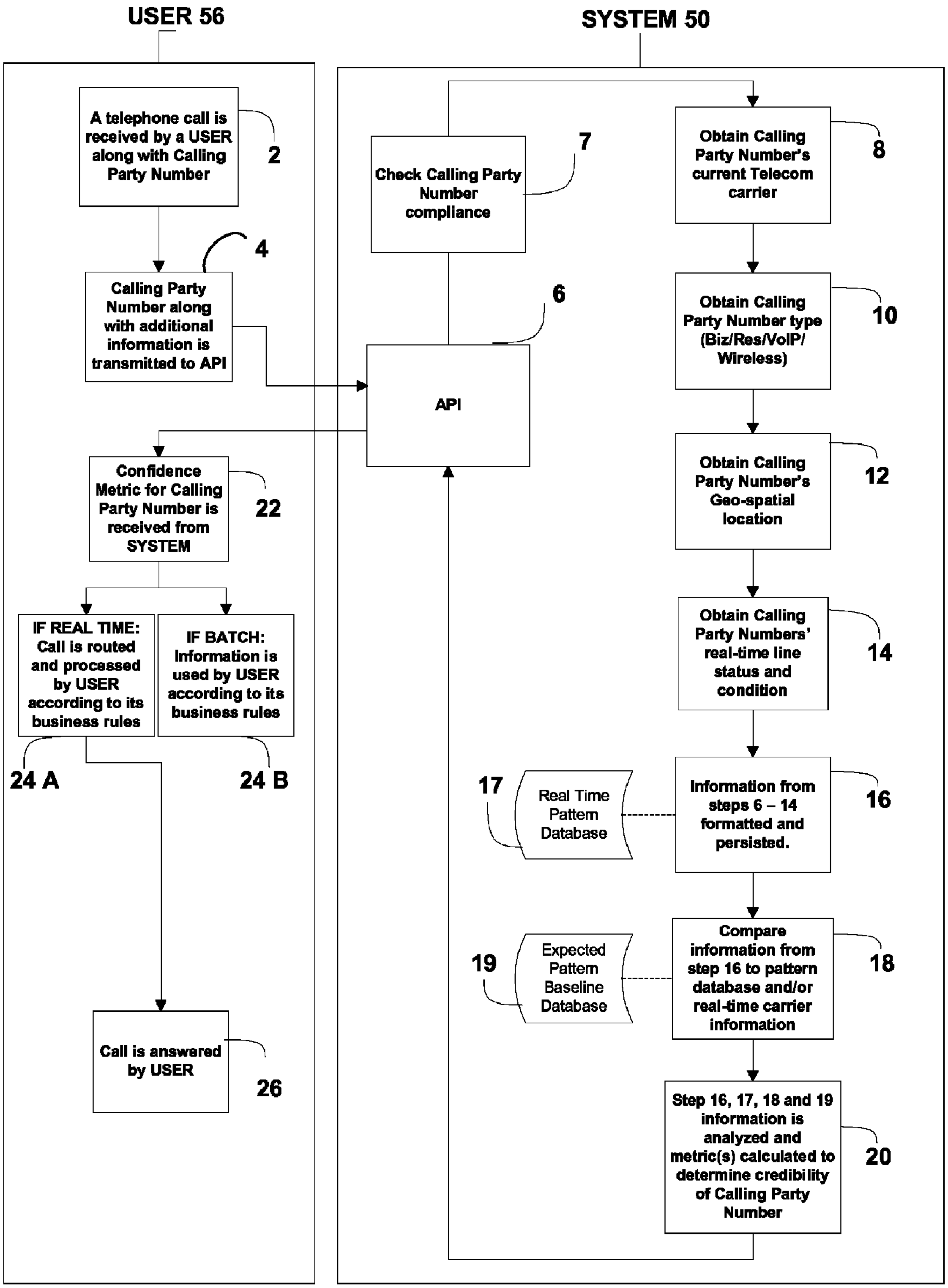

USER 56
SYSTEM 50
A telephone call is received by a USER along with Calling Party Number
2
Calling Party Number along with additional information is transmitted to API
4
Confidence Metric for Calling Party Number is received from SYSTEM
22
IF REAL TIME: Call is routed and processed by USER according to its business rules
IF BATCH: Information is used by USER according to its business rules
24 A
24 B
Call is answered by USER
26
Check Calling Party Number compliance
7
API
6
Obtain Calling Party Number's current Telecom carrier
8
Obtain Calling Party Number type (Biz/Res/VoIP/ Wireless)
10
Obtain Calling Party Number's Geo-spatial location
12
Obtain Calling Party Numbers' real-time line status and condition
14
Information from steps 6 – 14 formatted and persisted.
16
Real Time Pattern Database
17
Compare information from step 16 to pattern database and/or real-time carrier information
18
Expected Pattern Baseline Database
19
Step 16, 17, 18 and 19 information is analyzed and metric(s) calculated to determine credibility of Calling Party Number
20

FIG. 1

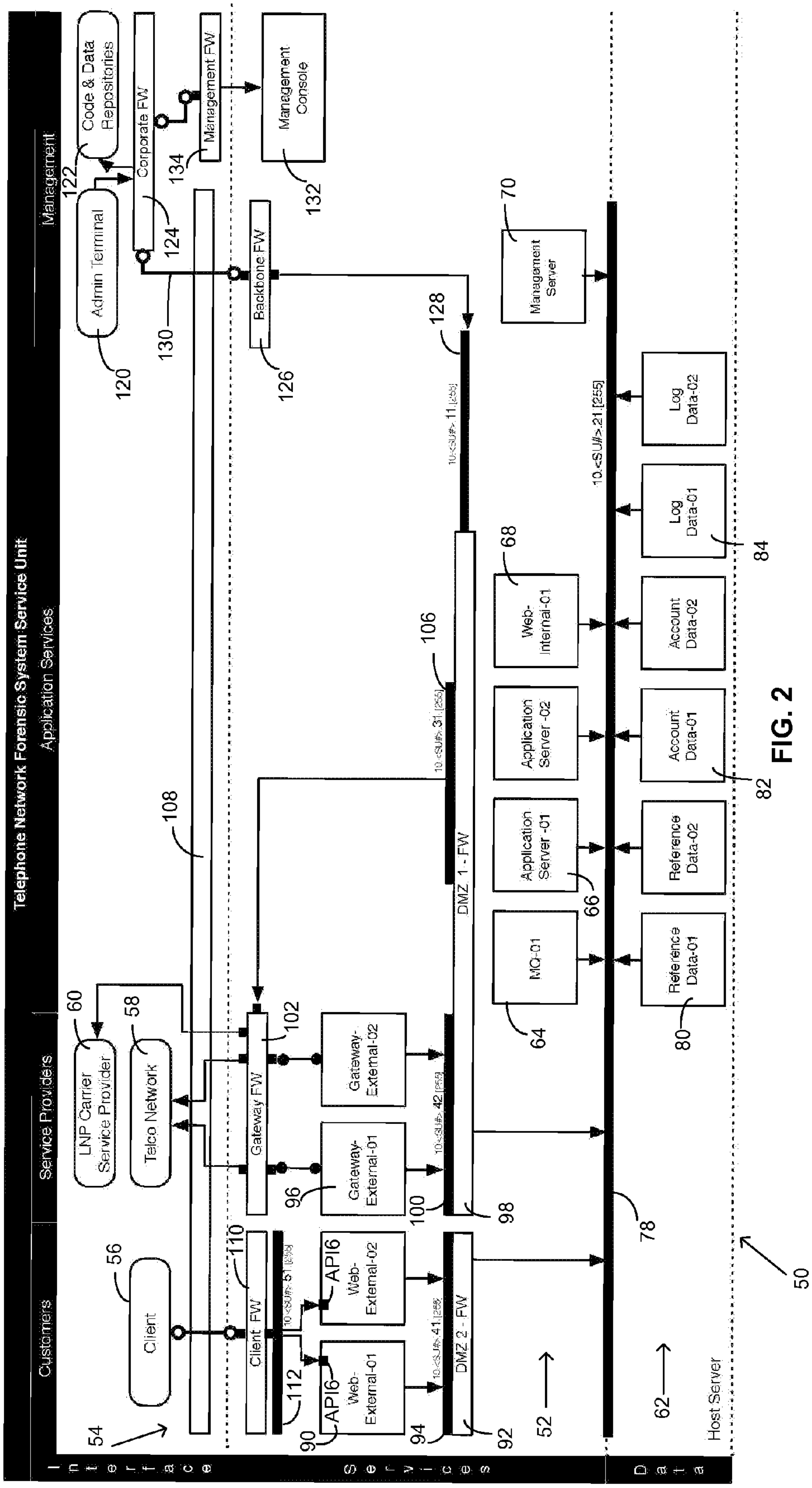

Telephone Network Forensic System Service Unit
Customers
Service Providers
Application Services
Management
Interface
Services
Data
Host Server
54
Client
56
LNP Carrier Service Provider
60
Telco Network
58
Admin Terminal
120
Code & Data Repositories
122
Corporate FW
124
130
Management FW
134
Management Console
132
Backbone FW
126
128
10.<SU#>.11.[255]
Management Server
70
10.<SU#>.21.[255]
Log Data-02
Log Data-01
84
Account Data-02
Account Data-01
82
Reference Data-02
Reference Data-01
80
Web-Internal-01
68
Application Server -02
Application Server -01
66
MQ-01
64
106
10.<SU#>.31.[255]
DMZ 1 - FW
108
Gateway FW
102
Gateway-External-02
Gateway-External-01
96
10.<SU#>.42.[255]
100
98
78
Client FW
110
10.<SU#>.51.[255]
API6 Web-External-02
API6 Web-External-01
112
90
10.<SU#>.41.[255]
DMZ 2 - FW
94
92
52
62
50

FIG. 2

METHOD OF AND SYSTEM FOR DISCOVERING AND REPORTING TRUSTWORTHINESS AND CREDIBILITY OF CALLING PARTY NUMBER INFORMATION

RELATED APPLICATION

This application claims benefit of U.S. Provisional Patent Application No. 61/179,629, filed May 19, 2009.

COPYRIGHT NOTICE

TECHNICAL FIELD

This disclosure relates to calls placed in telecommunication and information service networks and, in particular, to establishing, for call recipients, the credibility of incoming calls by discovery of and reporting on the credibility of Automatic Number Identification (ANI) information in-line with the incoming calls in progress.

BACKGROUND INFORMATION

ANI (Automatic Number Identification in North America is the 10-digit billing telephone number of the caller) was made available in 1967 to a business telephone customer for toll free circuits (800 or “Inward-WATS”) to inform the business telephone customer who was calling because the called business was paying the toll costs of the incoming call. ANI and Calling Number Identification (Caller ID) were made available as products to residential and small business telephone customers to provide them with the 10-digit telephone number of the calling party, and by the late 1980s in some cases the caller’s name. Businesses such as banks, call centers, and government entities such as 911 service centers have relied on ANI information as a factor in identity determination; as an element in location discovery; and for call routing assistance, workflow efficiency, and fraud mitigation.

The ability to falsify ANI has been available for over a decade, but only to sophisticated and mostly regulated telecommunications carriers and very large business Users subscribing to expensive multi-line Primary Rate Interface (PRI) telephone circuits. ANI control has a legitimate use. As an example, a large business uses ANI control to display its main telephone number on all outgoing calls from its multiple lines.

The ability to falsify ANI stems from interaction of new technologies with legacy telecommunications architecture. Before the advent of information services network (e.g., Internet) telephony and deregulation, the telecommunications network was a closed system with one or both of a limited number of trusted FCC- and Public Utility Commission-licensed telecommunications companies adhering to a finite set of standards. Telecommunications decentralization and deregulation, as well as Internet telephony (Voice over Internet Protocol (VoIP) technology), have exposed this legacy architecture to an abundance of new telephony products and services that inject calls and calling data from outside the control of the legacy telecommunications network. The telephony network then delivers to its destinations these calls and associated information, in most cases, without checking their validity. Consequently, this system supplies an opening for criminals to easily place calls with fabricated or “spoofed” ANIs for nefarious purposes. ANI fabrication or spoofing is a low cost, powerful penetration tool used to impersonate identity and location. Multiple companies and, more importantly, technologies exist for the sole purpose of enabling anyone, anywhere, to spoof ANI and Caller ID for pennies each call.

Throughout the past 25 years, telecommunication Users have relied on ANI and have built vital business processes around the incoming calling party telephone number. In addition, most businesses have developed sophisticated inbound telephone answering systems (known as IVR) that answer calls and are programmed with rules-based decision parameters grounded on the ANI. Now, relying on non-validated ANI undermines these critical marketing, technical, and security processes used for authentication, identity, location, and activation in today’s financial services, general business, and government enterprises. As one specific industry example, major financial institutions now have compromised critical operations that were built upon the trustworthiness of ANI. Applications such as bank-card activation, credit issuance, money transfers, new account applications, and customer service have all relied on the layer of security ANI has provided. Decisions made using the current non-validated ANI place an enterprise at risk of diminished revenue by limiting new product offerings and increased losses from fraud. Attempted fraud exceeds $50 billion each year in the U.S. alone. Identity fraud is the key driver in these losses. Today, more bank card activation fraud occurs by telephone than by other remote banking channels combined (i.e., not face-to-face), such as ATM, e-mail, and world wide web.

There are several ways in which a motivated individual can take advantage of the current state of the art to manipulate ANI. VoiceXML applications let Users change ANI and Caller ID. An open source PBX software application, such as Asterisk, allows users to manipulate ANI. Competitive service providers and telecommunication carriers can set their own ANI. Moreover, certain companies exist today for the sole purpose of allowing ANI and Caller ID to be spoofed and falsified. Businesses such as Camophone, Telespoof, Covert-Call, and dozens of others offer widely available ANI and Caller ID spoofing for pennies each call.

The consequences of prevalent, facile manipulation of ANI provide motivation to restore integrity to the use of ANI. One major consequence is financial fraud, which is on the rise and is driven primarily by identity fraud. Traditional financial services customer verification tools such as information-based authentication are being compromised. Most financial service companies use ANI as the apex identifier in their telephonic decision-making. If false trust is placed in spoofed ANI, downstream decisions are compromised. Decisions made using current non-validated ANI is placing companies at risk, limiting new product offerings, and increasing losses from fraud. The disclosed approach restores the value of ANI by reestablishing the security of telephone transactions.

There are more financial transactions conducted over the telephone than are conducted on the world wide web, even in today’s Internet pervasive environment. Of the more than two billion telephone calls placed annually to U.S. financial institutions alone, nearly all rely on ANI for security, location information, call routing, and identity authentication. Knowing the caller’s location or that the caller is in possession of an actual telephonic device is the foundation and an important factor for trusted telephone commerce.

A major nonfinancial consequence is criminal mischief. A Washington state man was sentenced to 30 months in prison, after using ANI spoofing to send SWAT teams to the houses of a dozen innocent, unknowing individuals.

The following is a chronological summary of the evaluation of ANI spoofing and legislative attempts to combat it.

In 2003, VoiceXML applications let Users change ANI, and, at the same time, VoIP telephony entered the marketplace. An open source PBX software application, called Asterisk, allows users to manipulate calling party number information. Asterisk is a software implementation of a telephone private branch exchange (PBX) originally created in 1999 by Mark Spencer of Digium. As an example, if the ANI field is left blank by the Asterisk or carrier switch, any user can easily manipulate the Caller ID information using Asterisk, thereby populating the ANI field with the same misinformation as the spoofed Caller ID. Asterisk allows Users to send spoofed ANI in the same way that businesses had been setting their ANI with PRI lines.

In 2004, a new ANI spoofing service, named Star38, (using VoIP and Asterisk) was launched and gained attention from worldwide mainstream media after USA Today published in its daily paper a front-page article about the service. The same year, others followed such as Camophone, Telespoof, and CovertCall. Over the next year, a dozen additional services started delivering ANI spoofing services.

By 2006, the FCC began investigations into these services, and the House of Representatives and the Senate considered several bills attempting to outlaw use of ANI spoofing for fraudulent purposes. ANI spoofing gained the attention of the mainstream media as SpoofCard announced the cancellation of an account belonging to Paris Hilton that was used to break into the voicemail of Lindsay Lohan to harass her.

On Jun. 27, 2007, the United States Senate Committee on Commerce, Science and Transportation approved and submitted to the Senate calendar Senate Bill S.704, which would have made spoofing ANI a crime. Titled the "Truth in Caller ID Act of 2007," the bill would have outlawed causing "any caller identification service to transmit misleading or inaccurate caller identification information" via "any telecommunications service or IP-enabled voice service." Law enforcement would have been exempted from the rule. A similar bill, HR251, was recently introduced and passed in the House of Representatives. It had been referred to the same Senate committee that approved S.704. The bill never became law because the full Senate never voted on it; it was added to the Senate Legislative Calendar under General Orders, but no vote was taken, and the bill expired at the end of the 110th Congress. On Jan. 7, 2009, Senator Bill Nelson (FL) and three co-sponsors reintroduced the bill as S.30, the Truth in Caller ID Act of 2009, which was the bill referred to the same committee in the Senate. The House of Representatives passed the Truth in Caller ID Act of 2010 in April 2010, but the bill has yet to be reconciled with the Senate version. The new bill states that Caller ID may not be spoofed to be intentionally misleading or inaccurate. No federal bill has yet to be signed into law. Several of the States have passed bills making misleading Caller ID spoofing illegal.

What is needed is a method to detect or report the accuracy and truthfulness of ANI.

SUMMARY OF THE DISCLOSURE

A method of and system for discovering and reporting the trustworthiness and credibility of calling party number information, such as Automatic Number Identification (ANI) or Calling Number Identification (Caller ID) information, or for inbound telephone calls entails use of real time telephone network status and forensics, network data, locally stored data, and predictive analytics. Practice of the disclosed method is neither detectable by nor intrusive to a calling party, and the method can be implemented into existing enterprise, information services, and telecommunications infrastructures.

The disclosed method performs ANI analysis with the calling party's telephone or telephonic device in a transitional state between an actual or a virtual on-hook condition and an answered condition, and is implemented as follows in a preferred system. When the first indication of an incoming call is detected by a User itself or equipment implementing an Application Programming Interface to communicate with the System, the ANI, along with other information such as the dialed number (DNIS) and incoming trunk identification information, is transferred to the System, using an Applications Programming Interface (API). The disclosed System quickly begins decomposing the calling party number (i.e., supposed telephone or billing number) to check the calling party number validity, check call velocity, compare the originating switch identifier with the NPA-NXX of the calling party number, and check other call number attributes. Calling party number validity relates to format issues for the North America Numbering Plan, such as, for example, whether the area code starts with an impermissible digit ("1" or "0") or whether the calling party number contains greater or fewer than 10 digits. Calling velocity relates to whether an excessive number of calls have been placed by a calling party to one or more Users within a specified unit time period. The NPA-NXX of a calling party number relates to the breakdown of 10-digit number, in which NPA refers to the three-digit numbering plan area (area code) and NXX refers to the three-digit central office (exchange) code.

If a specified one or number of such attributes suggest an anomalous or suspicious calling party number, the disclosed System determines noncompliance of the calling party number, and the System can terminate the procedure and indicate to the User that a calling party number is of low credibility. To continue the analysis of the calling party number, the disclosed System begins to discover the origins of the calling party number, such as telecommunications carrier, line type (e.g., business, government, residence), geo-location, network conditions, and network condition call progress message patterns. The System next begins to probe the calling party number by examining network signaling including call forward messages to ensure probing of the received calling party number and using the telecommunications network by calling and signaling to detect and record status, messages, line conditions (e.g., busy signal), hook switch status, answer and message timings, call forward actions and responses. The origins of the calling party number and the calling number network responses are used to create a real time pattern of all the above elements. The signaling and condition patterns represent, therefore, characteristic "thumbprint" patterns of the calling number telephone network and its call progress functions. The real time pattern is then compared against a historical database of expected call patterns of valid and invalid ANI decomposing processes. Based on the closeness of patterns and the degree of match, a confidence metric is calculated using statistical probabilities. The confidence metric is used by one or both of the User and the System to determine the validity of the ANI. Once the ANI is validated, the recipient can have a higher degree of confidence in the validity of the calling party number and place more trust in it.

The following presents examples of uses, and systems that would benefit from implementation, of the disclosed method.

In the banking industry sector, credit, debit, ATM, and gift cards are mailed to customers. When these cards are received by the recipient, most banks request that the recipient confirm receipt of the card by "activation" of the card. The most preferred method of activation entails placement of a call by a card recipient from his or her home telephone to a toll-free (800) number of the bank to activate the newly received card. The use of a toll-free (800) service by the bank ensures the transmission of ANI information to the bank, even if the consumer has a feature on his or her telephone line to "block Caller ID transmission." The transmitted ANI information is one factor used by the banks to prove that the card in fact is in the intended recipient's possession.

Banks can also use additional factors of,authentication to further identify and locate the caller by one or both of asking for personally identifiable information (PII) and relying on voice biometrics, primarily as a consequence of the now unsecured and "spoof able" nature of ANI. PII may be, for example, a social security number or date of birth. Using PII to conduct information-based authentication has its challenges and risks. Information based authentication using PII such as social security numbers or a mother's maiden names exposes the bank to additional risk. PII information is regulated, and, if the PII information in the bank's possession is lost or stolen from the bank, large costs and fines can be levied against the bank by government entities enforcing current data breach laws. Moreover, because of the high number of past data breaches, a very high percentage of consumers have had their PII data compromised already, making PII available to criminals for use in ID theft. (In 2009, the Identity Theft Resource Center reported 493 breaches and 300 million records exposed.) In addition, another aspect of PII access has further eroded the value of information-based authentication. Social networking websites such as FaceBook, LinkedIn, MySpace, Ancestry, Twitter, and dozens more all contain and share PII with the public, further de-valuing the use of PII knowledge as a tool for identity authentication. ANI is one of the authentication tools available to banks that are not PII based for telephone-based transactions. The disclosed method helps restore the value lost to spoofing and fraudulent ANI transmissions, providing a powerful new tool to banks to authenticate their customers by again using and trusting validated ANI as a factor in authentication for the telephone channel.

The disclosed method and system return the trust, credibility, and security to incoming telephone calls by discovering and reporting on inaccurate ANI information in-line with a call in progress, allowing trust to be correctly placed in real time that the ANI information has not been altered or set incorrectly or "spoofed" by the caller or a telecommunications carrier. The disclosed system and method can be used by business, government, and consumers alike, as well as provide an existing telecommunications carrier a tool to improve the security and value of its network.

Additional aspects and advantages will be apparent from the following detailed description of preferred embodiments, which proceeds with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINAS

FIG. **1** is a hybrid system process block and method step flow diagram of the disclosed method of and system for determining trustworthiness and credibility of calling number information relating to calls placed in a telecommunications network.

FIG. **2** is a block diagram of a telephone network forensic system service unit suitably configured to implement preferred methods of determining credibility of calling party number information performed in accordance with the hybrid process block and method step flow diagram of FIG. **1**.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In telephony, the calling party number information is delivered and described in many different ways. This document uses the acronym "ANI" to describe the following types of calling party number information systems and descriptions, unless any one of the following terms needs to be used specifically to communicate clearly: Caller ID or CID; Calling Party Number or CPN; Calling Number Identification (Identifier) or CNID; Calling Party Identification (Identifier) or CPI; Automatic Number Identification (Identifier) or ANI; Automatic Number Identification Information Digits or ANI II, ANI 2, ii digits; Billing (Billed) Number or BN; Caller (Calling) Line Identification or CLID; A-Number; and Calling Party or CP. The term "call" is used in this document to define any connection over a telecommunications or an information service network and includes, but is not limited to, landline, wireless, modem, facsimile, Session Initiation Protocol (SIP), and Voice over Internet Protocol (VoIP) transmissions.

The Problem the Disclosed Method and System Solve

With the deregulation and de-centralization of the telecommunications landscape and the introduction, proliferation, connection, and integration of information service network telephony (e.g., Internet VoIP) into the Public Switched Telephone Network (PSTN), combined with the ability to control the transmission of a caller's telephone number to a called party in the many forms (most commonly called ANI and Caller ID), is now controllable by the calling general public.

Before the dramatic marketplace changes outlined in this section, a calling party's number was securely transmitted by a regulated telecommunications company to the called party.

This newly found control of the telephone network by the public at large, mainly through use of VoIP connections, has caused the recipient of a telephone call to distrust in the accuracy and truthfulness of a calling party's telephone number.

The following description of implementations of preferred embodiments is presented with reference to FIG. **1**, which is a hybrid system process block and method step flow diagram. The diagram includes User related function blocks and system related process module blocks, as indicated in FIG. **1**.

An Incoming Call **2** block represents an event in which a called party (User) receives a telephone call delivered by a telecommunications carrier from a calling party. The carrier delivers an ANI, (usually 10 digits long in North America) along with or before the voice portion of that call is connected to the called party.

A Transmission **4** block represents a User (such as a bankcard activation center or a 911 emergency services call center) transmitting the ANI to the System before the call is answered and while the calling party hears one or more ringing tones. This transmission before the call is answered (goes off-hook) by the User enables the calling party's telephone to be in a more predictable and detectable transitional state. This transmission step may be performed through any conventional data transmitting technique, such as over the Internet with a virtual private network connection, a remote or private circuit connection, or a local area network using any data transmission model such as HTTPS, SOAP, or XML. This transmission step is not limited to offering only ANI information. For example, the User may transmit the time of day, trunk number, ANI II digits, dialed number information (DNIS), SIP header and routing information, transaction number, unique identifier, or other information or data that may be helpful to the System, or to the User if re-transmitted back to the User, for example, to assist in re-associating a transmission with the calling party's call.

An Application Programming Interface (API) **6** block represents the User of the System receiving the data and information described with reference to Transmission **4**, and then re-transmitting the data in a standardized format to the System. The System sends, to the User, data and information in a standard format that are described in a Determine **20** block of the System. API **6** could make format standardization of data in any known manner, including fixed field database structure, name/value pairs, XML, tab delimited, comma delimited, fixed width, or variable length. API **6** could make the subsequent transmission in any known manner, providing an electronic data connection to an active database or data management system such as Oracle or a proprietary or open source software program. The machine or computer may record the data on any known information storage device, including RAM, magnetic media (e.g., a hard disk drive), or any other electronic medium.

A Calling Party Compliance block **7** represents decomposition of the calling party number to check its validity, check call velocity, compare the originating switch identifier with the NPA-NXX of the calling party number, and check other call attributes. If it determines noncompliance of the calling party number, the System can terminate the procedure and indicate to the User that a calling party number is of low credibility. Otherwise, System operation proceeds as described below.

A Carrier Discovery **8** block represents a query of available network-accessible Local Number Portability (LNP) databases, such as the ones maintained by North American Numbering Plan Administration (NANPA), NetNumber, or TNS, to determine the current telecommunication carrier that services and owns the ANI number delivered in Transmission **4** from the incoming call placed to the called party in Incoming Call **2**. This query could be performed via the Internet using a secure TCP/IP protocol or other methods, such as Signaling System 7 (SS7), ATM, ITU-T, SIGTRAN, or Enum. In another variation, a locally stored database could be queried to determine the current telecommunication carrier that provisioned the line of the ANI from the incoming call placed to the called party in Incoming Call **2**.

A Line Type **10** block represents use of databases of telephone circuit types (such as, for example, business, wireless, residential, pay telephone, prison telephone, VoIP, satellite, pre-paid, post-paid, SIP, or pager) and information from other process modules or steps in the System such as Carrier Discovery **8** to assign a Line Type **10** to the ANI from Incoming Call **2**. A Line Type **10** database is created by assigning, analyzing, and building a compiled database of ANI Line Types from commercially available database(s) such as TargusInfo, InfoUSA, Acxiom, or others with databases maintained by telecommunication carriers or third party providers, such as Verizon, TNS, or NANPA, and from proprietary databases developed from primary research or housed on behalf of clients (numbers on which fraud has been previously committed or numbers assigned by the client as high risk). The compilation is performed by analysis of source quality metrics or other known techniques. These databases could be network (Internet, SS7) accessible or locally stored in the System or by combination. In another embodiment, Line Type **10** would be determined from a carriers business practices. Such an example would be Integra Telecommunications, which, at the time of this writing, provides only business line types.

Geo-location **12** block represents determination of the city and state, latitude, longitude, and other geospatial information about the ANI. The geo-location is determined by querying one or more databases, such as Telcordia, that provide routing guides using available rate center data providing geospatial data inferred from an ANI. International numbers can also be identified, using country-calling codes. Use of attribute data and vector data models collected, compiled, and analyzed for specific areas such as LATAs (Local Access Transport Areas) or a carrier's switch serving areas enables inference of discrete locations from the analysis of data contained in the attributes associated with each ANI.

In an alternative embodiment, the determination of the caller's location can also be made by use of the Home Location Register (HLR) or other carrier-based real time database to determine which switch or end office or what wireless telephone offices are managing the call, and then to calculate the location of that switch. In a second alternative embodiment, a third party geospatial technology or vendor such as Geografx can be used to provide the geo-location of the caller. In a third alternative embodiment, the determination of the callers location can also be made utilizing IP address information where available. Standards such as IPv6 define routable home IP address information that can be used to determine geo-location information. Geo-location may be returned as Geo-location **12** data that are used to determine the serving switch to assist in call pattern recognition and creation represented by a Storage **16** block, a Real-Time Pattern **17** block, a Compare **18** block, an Expected Patterns **19** block, and Determine **20** block.

A Network Condition **14** block represents placement by the System of one or more outbound calls to the telephone number represented by the received ANI in Incoming Call **2** before the incoming call to the User is answered, which is represented by a Call Answer **26** block. This enables the calling telephone line to be in a predictable and detectable state because call waiting and other features are unavailable at this time on most line types during this unanswered off-hook ringing state. These calls should be placed from a switch that uses SS7 services or with a VoIP service allowing for SIP and/or SIP-T messaging or other available network connection types to allow for the maximum amount of call progress messaging and maximum number of details to be recorded such as call forwarding and route information and status. Network condition, line-status, call progress information, and call progress messages and their associated timing information are collected in Network Condition **14**. The outbound call(s) query the current network condition of the telephone number (such as, for example, busy, ring then answer, call forward then answer, and ringing no answer). Such calls produce a series of conditions, each with a status and response with specific timing associated with each call progress message or network state.

In addition to network messages, available audio energy detection and determination methods are used, and the results are analyzed with the use of dedicated or shared digital signal processing (DSP) hardware and/or software to determine the type of answer condition and line type (such as a answering machine, fax machine, carrier-based voicemail, business line, automated attendant, or call progress tones including intercept tones, reorder tones, or guard tones). These status, conditions, and responses are categorized with associations and timings for later analysis performed in Determine **20**. In another variation, data connections (such as SS7 or virtual private network) to telecommunications providers may provide additional information as to the network condition of the ANI received in API **6**.

Connections to the telecommunications or third party provider may use new methods (such as real-time call detail record (CDR) analysis), existing methods (such as a CALEA interface or home location registers (HLR)), or billing ports and computer telephony interface (CTI) ports to access line status information. An example of the type of query and response in this variation would be to query a carrier through currently available means, such as a VPN, dedicated circuit, or SS7 connection, to determine whether a specific ANI is currently in a ringing state with the dialed number (DNIS) transmitted to the System in Transmission **4**. In another embodiment, the call status returned to the System from such query could be "in-progress" (answered) if the ANI was transmitted to the System in Transmission **4** after the call had been answered. In another embodiment, after the User receives the call in Incoming Call **2**, and after completion of Call Answer **26**, the User is informed that the System or another system managed by the User will be calling back the calling party while looking at real time network forwarding messages and other signaling after the current call terminates. This is done to verify that the received ANI transmitted in Incoming Call **2** is reachable by an outbound call and is, in fact, the number the User is using to place the call received in Incoming Call **2**. A new outbound call is then placed to the ANI in Incoming Call **2** to the calling party to verify that the calling party is in fact reachable at the number that was received in Incoming Call **2**. This outbound call is placed from a switch that uses SS7 services or with a VoIP service allowing for SIP-T messaging or other available network connection types. Such placement of the outbound call allows for the maximum amount of call progress messaging and number of details to be used by the System, so as to detect whether a call forward or other message is detected after the call is placed to the User, thus indicating the call was potentially not connected to the ANI from Incoming Call **2**.

Storage **16** represents sorting by network codes, condition, and timing the responses received from the outbound call(s) for storage and later analysis for validity, pattern recognition, and other risk factors by such elements as network condition, time of day, call progress messages, response times by carrier, variability in status messages, latency in telecommunications networks, and statistical probabilities. The analyzed responses are then sorted and formatted with all other data obtained in API **6**, Carrier Discovery **8**, Line Type **10**, Geo-location block **12**, and Network Condition **14** as patterns in a database represented by Real Time Patterns **17**.

In Real-Time Patterns database **17**, all the data from Storage **16** that were persisted as patterns are stored as a database for analysis, represented by Compare **18**. The following is an example of a valid ANI call pattern: a call placed to a Verizon (potentially Frontier) residential landline number that is in a previous GTE area in Oregon, does not have carrier-based voicemail activated as an optional feature, and is in an outbound ringing state will show as busy, while the same line that has carrier-based voicemail and call waiting features active on that line will show 1) a partial ring back message and then 2) an answer from the voicemail system within three seconds. In addition, the voice energy analysis and determination from the digital signal processing (DSP) would indicate that an answering device answered the call. In an invalid ANI call pattern, if it is determined that a human being answered, as taught by one or more complete ring cycles (six or more seconds after call is placed, with no call transfer message)

along with a digital signal processor DSP determination of "human" answer, or if a ring without an answer pattern occurs, then the calling party in Incoming Call **2** would not have been calling the User in Incoming Call **2** because the call waiting feature is disabled on this line type in an outbound ringing transitional state.

In Compare **18**, the pattern data stored in the Real-Time Patterns database **17** from Storage **16** are then compared against expected pattern results found in an Expected Patterns database **19**. One or more patterns will be retrieved from Expected Patterns **19** based on information from Carrier Discovery **8**, Line Type **10**, and Geo-location **12**. Patterns need not be exact to match between Expected Patterns database **19** and Real-Time Patterns database **17**. Matching logic indicating the closest comparable candidate between the Expected Patterns database **19** and the Real-Time Patterns database **17** is chosen as an input to the statistical probability calculation. The pattern recognition can take into account any statistical reference tables. For example, if a call is in an outbound ringing state, there is a high degree of probability that the calling party is in fact calling the User.

The Expected Patterns database **19** is composed of, but not limited to, baseline repeatable call flow patterns that are built in advance utilizing run-time, call statistics, hour usage and traffic patterns, and call frequency tables. The Expected Patterns **19** baseline database is created through empirical testing and sampling of known conditions in an advance of run-time process including placing multiple calls to a series of telephone numbers representative of the call handling process of each of the carriers throughout their network. The data include all SS7, VoIP, or wireless network messages, including their ordering and timing between messages. In addition, the Expected Patterns **19** data call patterns may be defined and recorded for each switch type and location within a carrier's network for valid ANI scenarios, then invalid ANI scenarios. The call patterns may include every message received from the network with their associated time and duration facts while placing a call, as well as messages received from the digital signal processing (DSP) monitoring and analysis during the call with associated time and duration facts, first for a valid ANI pattern call, then for an invalid ANI pattern call. These patterns are built, tested, and persisted for each unique combination of carrier (Carrier Discovery **8**) and line type (Line Type **10**), and optionally of geo-location (Geo-location **12**), as defined, for example, by serving switch. In addition to these elements, metadata are added to the call pattern data with elements such as time of day, frequency of recurrence, and statistical likelihood of call.

The Expected Patterns database **19** can be updated with each new ANI analysis while in run-time production, thereby creating a continuously learning system that provides ever-widening coverage of patterns. As part of the learning system, information stored in Storage **16** can be mined for additional information regarding new carrier information, new status, and new combinations of status messages and timing to be used to improve and enrich the Expected Patterns database **19**. This creates a learning system that benefits all steps, especially Determine **20**. The Expected Patterns database **19** will evolve through continued use of the System, adapting to telecommunications advances and creating a learning Expected Patterns database **19** with continuous feedback and updating.

In Determine **20**, the results from Compare **18** are analyzed for normalcy deviation and statistical match to patterns and their timing or duration between messages or conditions. This analysis entails comparing the real time patterns to previously expected call patterns of valid and invalid calling party decomposing processes to make a degree of match interpretation. In turn, these and other attributes or elements may be used to generate a score or metric of the validity of an ANI or, alternatively, as a singular determination such as "valid" or "invalid" or as a tiered system such as "red," "yellow," "green." Each additional attribute or element such as carrier, line type, geo-location, time of day, match of real time pattern to expected pattern is assigned a weighted value as factors of a confidence metric. A confidence metric is produced using statistical methods to indicate the probability that the ANI is correct. The metric can be adjusted by application or by recipient, based on previously defined thresholds. For example, a bank may consider a VoIP telephone to be of significantly higher risk, whereas a voicemail application requiring verification may consider a VoIP telephone to be of no more significant risk than a landline or wireless. Determine **20** then sends the metric along with other optional data as outlined in Transmission **4**, such as the time of day, trunk number, ANI II digits, dialed number information (DNIS), transaction number, or other information or data that may be helpful to the User, such as assisting in re-associating this transmission with calling party's call, is sent back to API **6**.

In another embodiment, analysis of call detail and other records by telephone number may also create new variables, including velocity of calls measured and metrics, to determine whether a telephone number or set of telephone numbers has been dialed excessively by an ANI, which could be one indication of a fraud pattern. The velocity measure over a period could be set by an application. As an example, more than 15 call requests in a 15-minute period may indicate a brute force attack and could be consider higher risk. This attribute would be an element used in the scoring and metric of accuracy and security of an ANI. In another embodiment, the System may gather additional information that may be useful to the User from additional systems, vendors, processes, or metadata from one or more of the steps taught in this application, such as caller name, address, city, state, zip code, latitude/longitude, equipment type, caller location, IP address, or other information, in addition to predictive scores or metrics such as a fraud score, risk score, credit score, marketing score, affinity score, expansion score, or warning indicators for bankruptcy, deceased, or information from a consortium database such as calling velocity to multiple locations within a specified time period, or known frauds, and then passed to API **6** along with the ANI validity metric.

A Metric Received **22** block represents receipt from API **6** of a confidence metric developed, scored, and created in Determine **20**, indicating the probability that the ANI from Incoming Call **2** is valid. API **6** sends such information to Metric Received **22** during the call (either pre-answer or post-answer) or at a later time (e.g., daily, weekly, or monthly), either individually or in aggregate in a batch data duration. Other data potentially received include optional data as outlined in Transmission **4**, such as the time of day, trunk number, ANI II digits, dialed number information (DNIS), transaction number or other information or data that may be helpful to the System or the User such as assisting in re-associating this transmission with calling party's call.

Processed **24**A and **24**B blocks represent alternative processing of the metric and other information taught in Metric Received **22**. The information delivered to and processed by Processed **24**A is analyzed, scored, and acted upon in real time. This processing is performed according to a set of rules and processes by the User or by a third party rules engine such as ALI or any other commercially available system or any proprietary system that routes or makes decisions on the handling of any call, caller or call flow, in accordance with the recipient's algorithm, to the proper queue or IVR or agent, along with other fraud or call processing rules or procedures. The User's telephonic business rules engine may provide additional call scripting based on one or both of the metric and the additional information provided from the System or the User's business rules. The information delivered to and processed by Processed **24**B is analyzed, scored, and acted upon as a batch process at, for example, the close of a business day. The processing is performed according to a set of rules and processes by the User or by a third party rules engine, as described above for Processed **24**A.

A Call Answer block **26** represents answering by User of the call by an off hook or supervision signal or by data packet sent to the Users' providing telecommunications carrier. The call is then processed.

Relationship, Flow and Logic Between the Steps, Methods and Elements

The preferred relationship among elements, including preferred logic and chronological order, is shown in FIG. **1**. The System performs ANI analysis to determine credibility of calling party information as the calling party's telephone or telephonic device is in a transitional state between an actual or a virtual on-hook condition and an answered condition. The System process preferably begins at Transmission **4** and ends at API **6**. As shown in the diagram, Transmission **4** preferably occurs before API **6**, which preferably occurs before Carrier Discovery **8**, and so forth. However, the order of many of these steps may be changed. By way of example but not limitation, Line Type **10** may occur during or before Carrier Discovery **8**, or during, or before Geo-location **12**: Moreover, Network Condition **14** could occur during or before either or both of Carrier Discovery **8** and Line Type **10**, as long as sufficient time remained to make the proper decision at Determine **20** before Call Answer **26**.

In another embodiment, Carrier Discovery **8**, Line Type **10**, Geo-location **12**, further, even Network Condition **14** could be altered or adjusted so that, if the data received in Line Type **10** were "prison telephone" or "pay-telephone," Carrier Discovery **8**, Geo-locate **12**, Network Condition **14** could be skipped or Geo-locate **12** could be preformed to verify the accuracy of data at Line Type **10** before moving to Network Condition **14** through Metric Received **22**.

In another embodiment, the System may be implemented using software running on a local machine at the location of the User and incorporated into its own processes could use the disclosed method taught here to achieve the same trustworthiness and validity metric. This System can be envisioned as a hosted solution, with software installed on client's computer system having associated databases and network connections, or alternatively, as a hardware appliance, prepackaged server, or system including the System and necessary equipment to function installed on client premises. The solution may be a combination of the above-mentioned deployment options.

FIG. **2** is a block diagram illustrating a preferred telephone network forensic System **50** that uses telecommunication links to establish information request and data information communication paths among a User, a telecommunications network, and external data sources to determine credibility of calling party number information of an incoming call to the User. System **50** is configured with a services layer **52** that provides core application services in the credibility analysis of ANI of a call placed to a User. Services layer **52** is linked to an interface layer **54** to receive messages from a Client or User **56** requesting ANI processing and to communicate with a telecommunications network **58** to access call information data or place a test call to the supposed calling party number and an LNP carrier service provider **60** to access call information data. (Process blocks **2**, **4**, **22**, **24**A, **24**B, and **26** shown in FIG. **1** relate to actions performed by or presented to User **56**.) Services layer **52** is also linked to a data layer **62** for access to internally stored call information data used to analyze ANI.

Services layer **52** includes a message queue server **64** and an application server **66** that process incoming call ANI verification requests. Message queue server **64** receives incoming ANI and delivers the results obtained by operation of application server **66**. Message queue server **64** supports the infrastructure for scalability and operational flow of System **50**. Application system server **66** fulfills a call verification request directed by message queue server **64** by controlling and coordinating the ANI processing steps performed as outlined in FIG. **1**. Message queue server **64** has an address to which all other servers provided in System **50** can direct requests for various processing tasks. Thus, the other servers in System **50** request information or deliver data through message queue server **64**, which routes data and queries for processing by the appropriate system servers. This message queue server **64**-centric architecture permits expansion of System **50** without disruption of operations of other system servers. A web internal server **68** runs queries through services layer **52** to perform internal test applications and emulate system performance without access to or by systems external to System **50**. A management server **70** performs an administrative function of monitoring the overall system operational status (e.g., checking for faults in ANI processing) of servers in services layer **52** and data layer **62**.

Services layer **52** is linked through a virtual switch **78** to data layer **62**, which includes a reference data server **80** that contains a carrier database of internal information about operational and organizational characteristics for commercially accessible telecommunication carriers, valid NPA-NXX codes, valid NPA-NXX codes as to geo-location, line type, and other information characterizing proper ANI. (Process blocks **7**, **10**, and **12** shown in FIG. **1** relate to cooperative actions performed by application server **66** and reference data server **80**.) An account data server **82** contains User account configuration information, and a log data server **84** tracks all transactions performed biSystem **50** for billing services, analysis, troubleshooting, and call progress message pattern updates. (Process blocks **16**, **17**, **18**, and **19** shown in FIG. **1** relate to cooperative actions performed by application server **66**, reference data server **80**, and account data server **82**.)

Services layer **52** and interface layer **54** are linked by multiple communication paths. Specifically, services layer **52** is linked to a web external server **90** through a firewall **92** and virtual switch **94**, to a gateway external server **96** through a firewall **98** and virtual switch **100**, and to a gateway firewall **102** through firewall **98** and virtual switch **106**. These firewall-virtual switch combinations provide secure interface within services layer **52** and from interface layer **54** to services layer **52** and data layer **62**. A User **56** located outside System **50**, as indicated by outside world boundary **108**, accesses System **50** through a client firewall **110** and virtual switch **112** to transmit to web external server **90** ANI associated with an incoming call verification request and to receive from web external server **90** results obtained after system processing of the ANI. The results obtained include a calculated confidence metric representing the credibility of the calling party number (FIG. **1**, process block **20**). Applications Programming Interface **6** is implemented by web external server **90** and defines a standard format by which communication takes place between web external server **90** and User **56**. Services layer **52** interfaces with telecommunications network **58** (FIG. **1**, process block **14**) through gateway external server **96**, firewall **98** and a virtual switch **100**, and gateway firewall **102** to place a test call to the supposed calling party number of the incoming call to User **56**. Services layer **52** interfaces with LNP carrier service provider **60** (FIG. **1**, process block **8**) to access (sometimes by purchase) call information data and to return accessed data to message queue server **64** through application server **66**, to virtual switch **78** and firewall **98**, through virtual switch **106** and gateway firewall **102**.

An administrative terminal **120** and associated code and data repositories **122** are linked through a corporate firewall **124** at interface layer **54** to System **50** and are routed to services layer **52** through a backbone firewall **126** and virtual switch **128**. This administrative link to System **50** allows corporate level management access, from across outside world boundary **108**, to System **50** via a secure link **130** to, for example, perform demonstrations of system functionality and obtain operational status of System **50**. A management console **132** in services layer **52** links administrative terminal **120** through a management firewall **134** to run the virtualization software of System **50**.

FIG. **2** shows six servers in duplicate to indicate operational, equipment, and virtual appliance redundancy to ensure continuing service in the event of localized failure of any one of the six servers of System **50**.

Basic and Optional Elements of Disclosed Method and System

The System can be implemented with all, part, or limited functionality of any method or step taught in this patent application or any combination. For instance, if User is interested only in validation of the ANI of wireless callers, and the LNP information learned in Carrier Discovery **8** is known to only provision wireless services, the Line Type **10** and possibly method Geo-Location **12** may not be required.

For situations in which the System had direct access to real time line status information by connections to carriers to disclose line status as taught is the first variation in Network Condition **14**, the requirement to perform additional network status queries may not be required.

Another system benefitting from implementation of the disclosed method is telephones used by consumers or individuals at work. Frequently today, consumers and individuals at work are relying on Caller ID information to determine who is calling them. This is increasing important with a relatively new and disturbing trend called Phishing. Phishing is a practice of fraudulently taking on the persona of an institution, such as a bank, for the purpose of defrauding a consumer or an individual at work. As an example, a person receives a telephone call, and his or her Caller ID device displays “Bank of ABC.” The “Bank” has called to verify credit card transactions for the security of the cardholder. The true caller is, however, in Eastern Europe and has no affiliation with Bank of ABC, but has simply used Caller ID spoofing to defraud the call recipient into believing his or her bank has placed the call. If the consumers or individuals at work fall prey to this fraud, the called person may share Personally Identifiable Information (PII) with the fraud perpetrator, allowing the fraud perpetrator to do financial harm by using the newly acquired PII from the victim. The disclosed method helps mitigate this fraudulent and costly practice.

It will be obvious to those having skill in the art that many changes may be made to the details of the above-described embodiments without departing from the underlying principles of the invention. The scope of the present invention should, therefore, be determined only by the following claims.

The invention claimed is:

1. A method of determining a source origin confidence metric of a calling party number or billing number associated with an incoming call from a telephonic device, comprising:

receiving the calling party number or billing number;

after receiving the calling party number or billing number and before the incoming call is answered, gathering operational status information associated with the calling party number or billing number, wherein gathering operational status information includes placing an outgoing call to the calling party number or billing number and receiving call progress messages associated with the outgoing call; and

determining the source origin confidence metric for the calling party number or billing number.

2. The method of claim **1**, further comprising receiving characteristics of the incoming call.

3. The method of claim **2**, wherein characteristics of the incoming call include one or more of time of day, trunk number, ANI II digits, dialed number information, an identifier of an originating switch, SIP Header information, SIP routing information, transaction number, call frequency indicator, SS7 data or a unique call identifier.

4. The method of claim **1**, further comprising determining whether the format of the calling party number or billing number is valid.

5. The method of claim **4**, further comprising upon determining that the format of the calling party number or billing number is invalid, generating a message that indicates the calling party number or billing number is invalid.

6. The method of claim **1**, further comprising obtaining a number of calls within a given timeframe that have been originated from the calling party number or billing number.

7. The method of claim **6**, further comprising determining whether the number of calls within a given timeframe that have been originated from the calling party number or billing number exceeds a threshold.

8. The method of claim **7**, further comprising upon determining that the threshold has been exceeded, generating a message that indicates the calling party number or billing number is invalid.

9. The method of claim **1**, further comprising determining a carrier associated with the calling party number or billing number.

10. The method of claim **3**, further comprising determining whether an NPA-NXX of the calling party number or billing number or whether the calling party number or billing number is associated with the originating switch.

11. The method of claim **10**, further comprising upon determining that the NPA-NXX of the calling party number or billing number or that the calling party number or billing number is not associated with the originating switch, generating a message that indicates the calling party number or billing number is invalid.

12. The method of claim **1**, further comprising:

determining a line status for the calling party number or billing number.

13. The method of claim **12**, further comprising when the line status for the calling party or billing number is determined to be answered, detecting audio energy to determine an answer condition.

14. The method of claim **13**, further comprising upon determining the answer condition to be a human answer, generating a message that indicates the calling party number or billing number is invalid.

15. The method of claim **12**, further comprising upon determining the answer condition to be ringing with no answer, generating a message that indicates the calling party number or billing number is invalid.

16. The method of claim **1**, further comprising generating a call pattern for the outbound call.

17. The method of claim **16**, wherein the call pattern includes data on timing between call progress messages.

18. The method of claim **16**, wherein the outbound call pattern includes one or more of network conditions, line-status, call progress information, call progress messages, answer conditions, and timing of call progress messages.

19. The method of claim **16**, wherein determining the source origin confidence metric of the calling party number or billing number is based on a comparison of the outbound call pattern to stored call patterns, characteristics, or both.

20. The method of claim **19**, further comprising:

identifying stored call patterns, characteristics, or both to be compared to the outbound call pattern based on one or more of line type, carrier, geo-location, or signaling patterns of the calling party number or the billing number.

21. The method of claim **1**, wherein the source origin confidence metric is a probability that the calling party number or the billing number is valid.

22. The method of claim **1**, wherein the source origin confidence metric indicates either the calling party number or the billing number is valid or invalid.

23. The method of claim **1**, wherein the source origin confidence metric indicates a calling party number or billing number validity indicator, wherein the validity indicators comprise a static set of predetermined indicators.

24. The method of claim **23**, wherein the set of predetermined indicators are red, green or yellow.

25. The method of claim **1**, further comprising:

adjusting the source origin confidence metric based on personal risk factors of an entity associated with the calling party number or billing number.

26. The method of claim **25**, wherein the personal risk factors include one or more of fraud score, risk score, credit score, marketing score, affinity score, expansion score, or warning indicators for bankruptcy, or whether a person associated with the calling party number or billing number is deceased.

27. The method of claim **25**, further comprising:

retrieving consortium information from an external database.

28. The method of claim **27**, wherein the external database includes data such as calling velocity to multiple locations within a specified time period for the calling party number or billing number, or known fraudulent calling party numbers or billing numbers.

29. The method of claim **16**, further comprising updating a stored call patterns database based on the outbound call pattern.

30. The method of claim **1**, further comprising:

providing the source origin confidence metric to an entity receiving the incoming call.

31. The method of claim **30**, wherein the source origin confidence matrix is provided to the entity receiving the incoming call in real-time or in batch mode.

32. A system for performing forensic analysis on calling party number information associated with an incoming call from a telephonic device, before the incoming call is answered, comprising:

an interface for receiving calling party number information associated with the incoming call;

a memory configured to store a plurality of expected call patterns; and

one or more processors configured to:

gather operational status information associated with the calling party number information, and

assign a source origin confidence metric to the calling party number using the operational status information and an expected call pattern in the plurality of expected call patterns.

33. The system of claim **32**, wherein the interface is further configured to receive characteristics associated with the incoming call.

34. The system of claim **33**, wherein the characteristics of the incoming call include one or more of trunk number, identifier of an originating switch, or transaction number.

35. The system of claim **32**, wherein the processor is further configured to derive characteristics of the incoming call.

36. The system of claim **35**, wherein the derived characteristics of the incoming call include one or more of carrier, geo-location of the call, or line type of the telephone device originating the incoming call.

37. The system of claim **36**, wherein the processor is further configured to select the expected call pattern based on the derived characteristics of the incoming call.

38. The system of claim **32**, wherein the calling party information includes the calling party number or billing number.

39. The system of claim **38** further comprising:

a device for initiating an outbound call to the calling party number or billing number.

40. The system of claim **39** further comprising:

a module for monitoring a set of call progress messages associated with the outbound call to the calling party.

41. The system of claim **40**, wherein the processor is further configured to generate a call progress pattern based on the set of monitored call progress messages.

42. The system of claim **41**, wherein the call progress pattern includes data on timing between call progress messages in the set of monitored call progress messages.

43. The system of claim **40**, wherein the processor is further configured to compare the call progress pattern to the expected call pattern to determine the source origin confidence metric for the calling party number or the billing number.

44. The system of claim **32**, wherein the operational status information includes a line status for the calling party number or billing number.

45. The system of claim **44**, further comprising:

an audio energy detector configured to determine an answer condition associated with the line status.

46. The system of claim **38**, wherein the source origin confidence metric is a probability that the calling party number or billing number is valid.

47. The system of claim **38**, wherein the source origin confidence metric indicates either the calling party number or billing number is valid or invalid.

48. The system of claim **38**, wherein the source origin confidence metric indicates a calling party number or billing number validity indicator, wherein the validity indicators comprise a static set of predetermined indicators.

49. The system of claim **48**, wherein the set of predetermined source origin confidence metric indicators include red, green or yellow.

50. The system of claim **38**, wherein the processor is further configured to adjust the source origin confidence metric based on personal risk factors of an entity associated with the calling party number or billing number.

51. The system of claim **50**, wherein the personal risk factors include one or more of fraud score, risk score, credit score, marketing score, affinity score, expansion score, or warning indicators for bankruptcy, or whether a person associated with the calling party number is deceased.

52. The system of claim **32**, further comprising one or more storage devices configured to store expected call patterns.

* * * * *

Exhibit 3

US009871913B1

(12) **United States Patent**
Saitawdekar et al.

(10) **Patent No.: US 9,871,913 B1**
(45) **Date of Patent: *Jan. 16, 2018**

(54) **SYSTEMS AND METHODS TO IDENTIFY ANI AND CALLER ID MANIPULATION FOR DETERMINING TRUSTWORTHINESS OF INCOMING CALLING PARTY AND BILLING NUMBER INFORMATION**

(71) Applicant: **TrustID, Inc.**, Lake Oswego, OR (US)

(72) Inventors: **Shreyas Dattatraya Saitawdekar**, Portland, OR (US); **Patrick Michael Cox**, Newberg, OR (US); **Daniel Vincent Stone**, Portland, OR (US); **Dean Franklin Black**, Vancouver, WA (US); **Richard J. Green**, Portland, OR (US)

(73) Assignee: **TrustID, Inc.**, Lake Oswego, OR (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/045,020**

(22) Filed: **Feb. 16, 2016**

Related U.S. Application Data

(63) Continuation of application No. 13/355,135, filed on Jan. 20, 2012, now Pat. No. 9,264,536.

(51) **Int. Cl.**

H04M 3/42	(2006.01)
H04M 3/436	(2006.01)

(52) **U.S. Cl.**
CPC ***H04M 3/42059*** (2013.01); ***H04M 3/436*** (2013.01); *H04M 2203/6045* (2013.01)

(58) **Field of Classification Search**
CPC H04M 3/42059; H04M 3/436; H04M 2203/6045; H04M 1/66; H04M 3/42068
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,754,475	A	6/1988	Pintos et al.
4,796,292	A	1/1989	Thomas
5,699,416	A	12/1997	Atkins
5,963,625	A	10/1999	Kawecki et al.

(Continued)

OTHER PUBLICATIONS

Saitawdekar et al., U.S. Appl. No. 13/355,135, filed Jan. 20, 2012, Office Action Communication, dated Dec. 20, 2012, 18 pages.

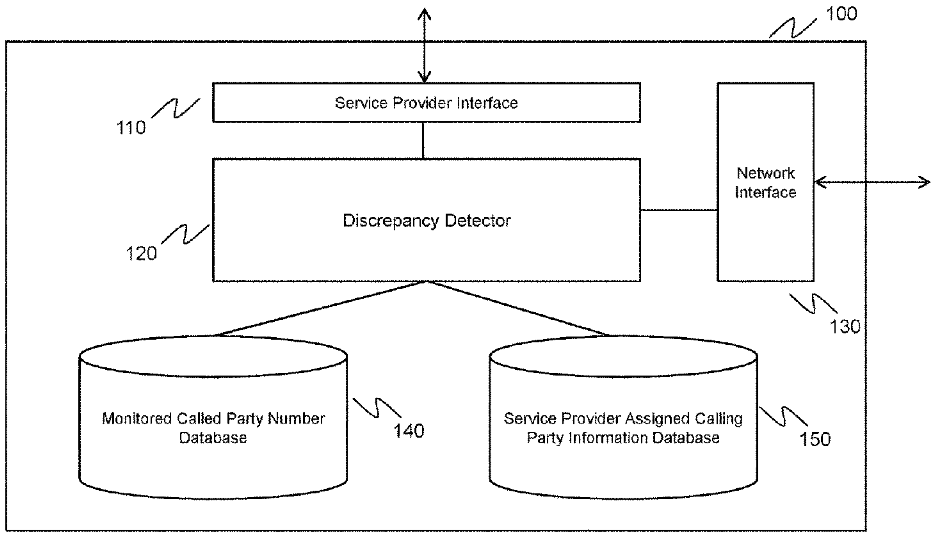
(Continued)

Primary Examiner — Sonia Gay
(74) *Attorney, Agent, or Firm* — Sterne, Kessler, Goldstein & Fox, P.L.L.C.

(57) **ABSTRACT**

Systems and methods for determining the trustworthiness of calling party information, such as caller ID and ANI information, contained in a call request are provided. The method includes receiving a call request at a service provider network element, such as a telecommunication carrier switch. A decision is made as to whether the call request should be verified by reviewing a database of called telephone numbers for monitoring. When the call request is to be verified, a determination is made whether a discrepancy exists between the calling party information contained within the call request and authenticated stored calling party information. For example, the caller ID information in a call request is compared to service provider caller ID information for the calling party to determine if they match. When a discrepancy exists, a discrepancy report is transmitted to the called party.

20 Claims, 4 Drawing Sheets


100
Service Provider Interface
110
Discrepancy Detector
120
Network Interface
130
Monitored Called Party Number Database
140
Service Provider Assigned Calling Party Information Database
150

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,307,926	B1	10/2001	Barton et al.
6,373,930	B1	4/2002	McConnell et al.
6,947,532	B1	9/2005	Marchand et al.
7,043,241	B1	5/2006	Sladek et al.
7,912,192	B2	3/2011	Kealy et al.
8,238,532	B1	8/2012	Cox et al.
8,254,541	B2	8/2012	Cai
2007/0121851	A1	5/2007	Maropis et al.
2007/0127658	A1	6/2007	Gruchala et al.
2007/0201660	A1	8/2007	Lan et al.
2007/0271339	A1	11/2007	Katz
2010/0166160	A1	7/2010	Moss et al.

OTHER PUBLICATIONS

Saitawdekar et al., U.S. Appl. No. 13/355,135, filed Jan. 20, 2012, Office Action Communication, dated Sep. 26, 2013, 16 pages.

Saitawdekar et al., U.S. Appl. No. 13/355,135, filed Jan. 20, 2012, Office Action Communication, dated Aug. 5, 2014, 14 pages.

Saitawdekar et al., U.S. Appl. No. 13/355,135, filed Jan. 20, 2012, Office Action Communication, dated Feb. 23, 2015 pages.

Saitawdekar et al., U.S. Appl. No. 13/355,135, filed Jan. 20, 2012, Notice of Allowance Communication, dated Oct. 6, 2015, 8 pages.

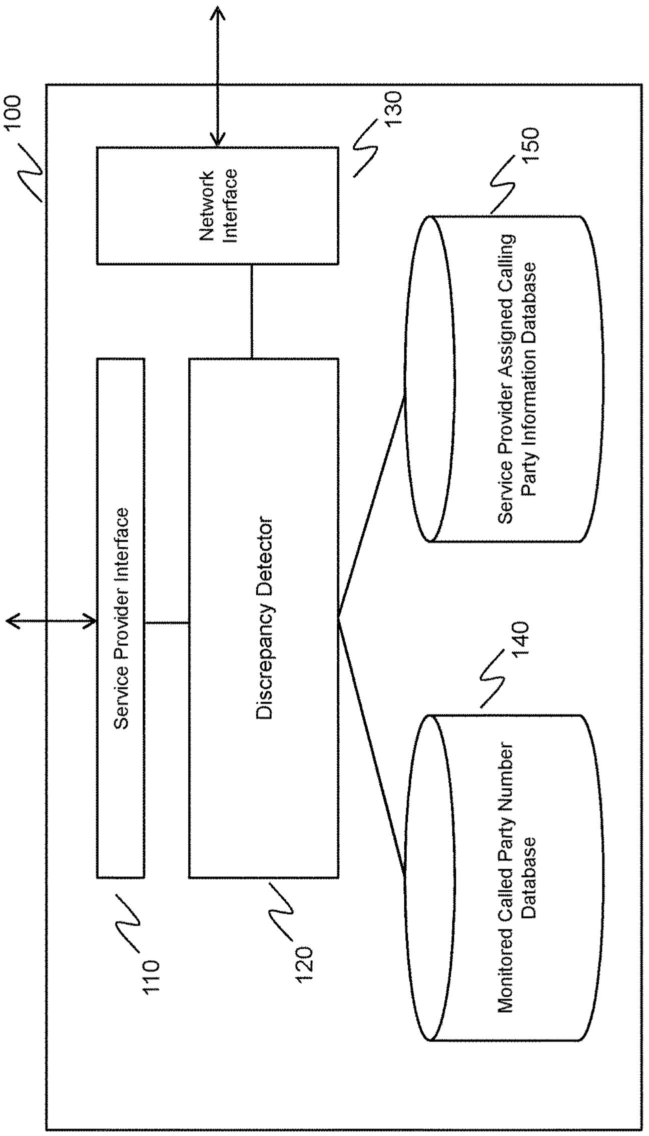

100
Network Interface
130
150
Service Provider Assigned Calling Party Information Database
Service Provider Interface
Discrepancy Detector
140
Monitored Called Party Number Database
110
120

FIG. 1

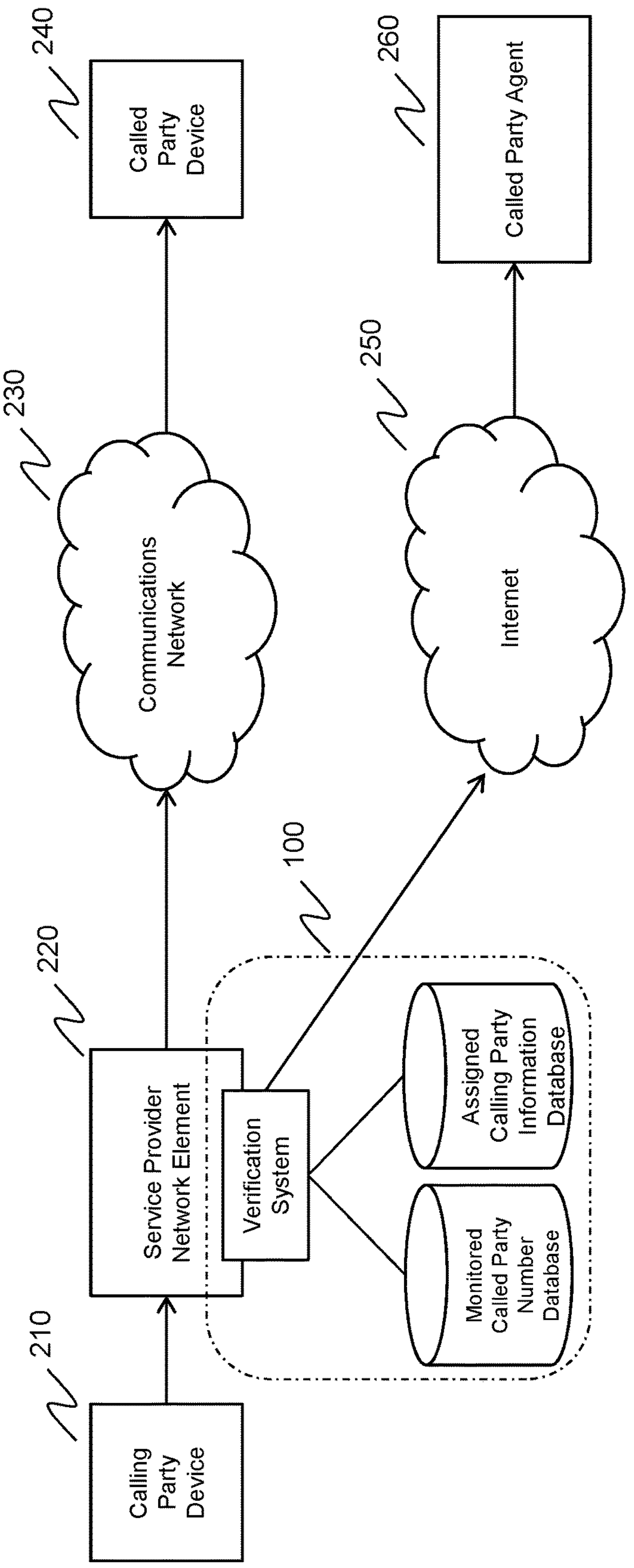

Calling Party Device
210
Service Provider Network Element
220
Verification System
100
Monitored Called Party Number Database
Assigned Calling Party Information Database
Communications Network
230
Called Party Device
240
Internet
250
Called Party Agent
260

FIG. 2

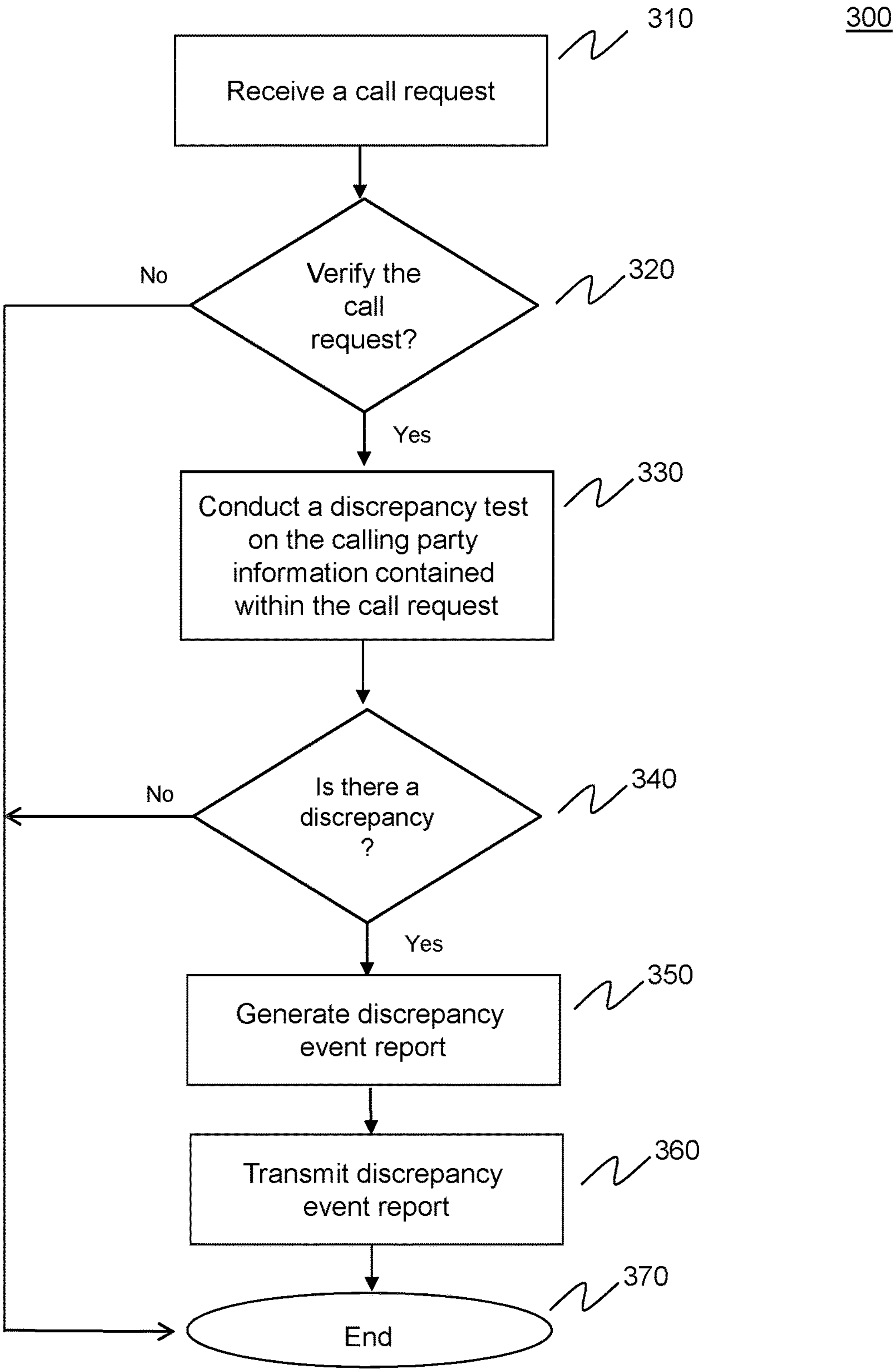

300
310
Receive a call request
Verify the call request?
320
No
Yes
Conduct a discrepancy test on the calling party information contained within the call request
330
Is there a discrepancy ?
340
No
Yes
Generate discrepancy event report
350
Transmit discrepancy event report
360
End
370

FIG. 3

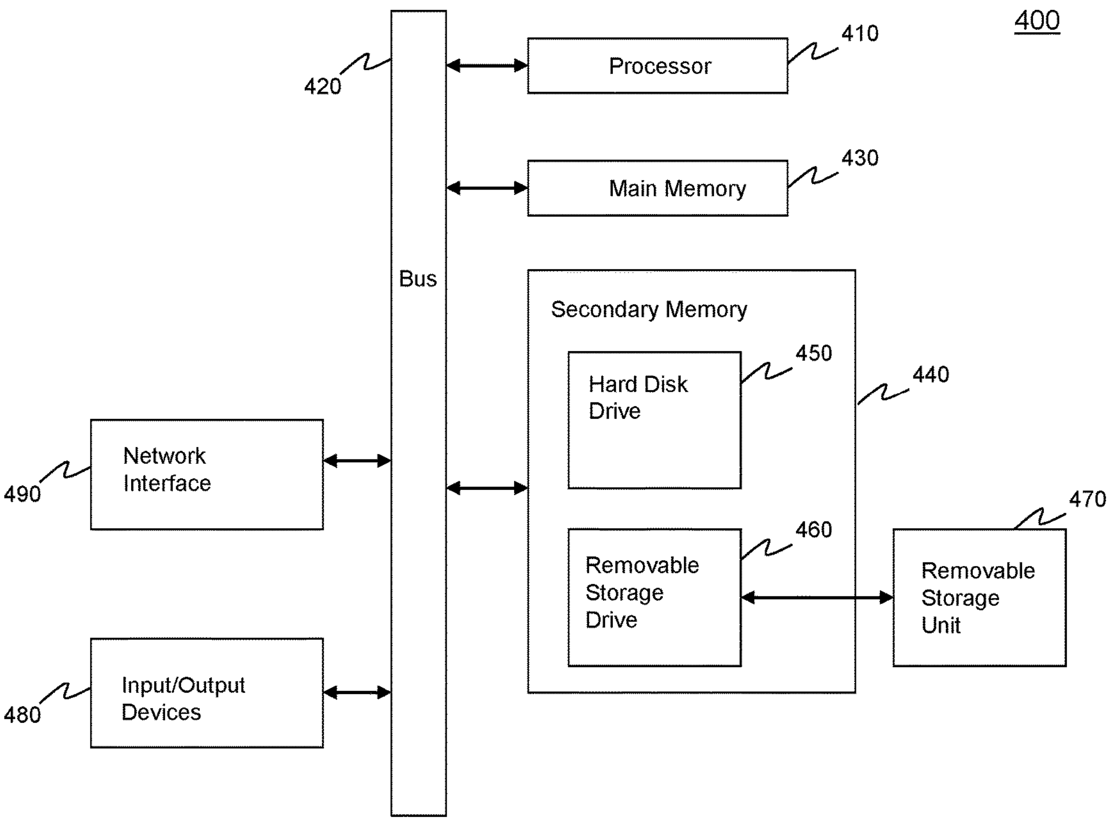

400
Processor
410
420
Main Memory
430
Bus
Secondary Memory
Hard Disk Drive
450
440
Network Interface
490
Removable Storage Drive
460
470
Removable Storage Unit
Input/Output Devices
480

FIG. 4

SYSTEMS AND METHODS TO IDENTIFY ANI AND CALLER ID MANIPULATION FOR DETERMINING TRUSTWORTHINESS OF INCOMING CALLING PARTY AND BILLING NUMBER INFORMATION

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of U.S. patent application Ser. No. 13/355,135, filed Jan. 20, 2012 (now U.S. Pat. No. 9,264,536), which is hereby incorporated by reference in its entirety.

BACKGROUND OF THE INVENTION

Copyright Notice

Field of the Invention

The present invention relates generally to calls placed in telecommunication and information service networks and, in particular, to establishing the credibility of incoming calls by identifying and reporting on the credibility of Automatic Number Identification (ANI) information and caller ID information.

BACKGROUND ART

Automatic Number Identification (ANI) in North America is information identifying the 10-digit billing telephone number of a caller provided to the recipient of the call. ANI was made available in 1967 to business telephone customers who purchased toll free circuits (800 or "Inward-WATS") to inform a business telephone customer who was calling, because the called business was paying the toll costs of the incoming call. ANI and Calling Number Identification (Caller ID) were made available as products to residential and small business telephone customers to provide them with the 10-digit telephone number of the calling party. Additionally, by the late 1980s calling name services were also made available in which a caller's name would be also delivered to a called party. Businesses such as banks, call centers, and government entities, such as 911 service centers have relied on ANI information as a factor in identity determination and as an element in location discovery. ANI information is also used for call routing assistance, workflow efficiency, and fraud mitigation.

The ability to control or manipulate ANI and caller ID information has been available for over a decade. Historically, only sophisticated and mostly regulated telecommunications carriers and very large business users, who subscribed to expensive multi-line Primary Rate Interface (PRI) telephone circuits had the ability to manipulate ANI. ANI control has legitimate uses. As an example, a large business uses ANI control to display its main telephone number on all outgoing calls from its multiple lines, rather than each of the individual lines.

The ability to falsify ANI and caller ID information stems from interaction of new technologies with legacy telecommunications architecture. Before the advent of information services network (e.g., Internet) telephony and deregulation, the telecommunications network was a closed system with one or both of a limited number of trusted FCC- and Public Utility Commission-licensed telecommunications companies adhering to a finite set of standards. Telecommunications decentralization and deregulation, as well as Internet telephony (e.g., Voice over Internet Protocol (VoW) technology), have exposed this legacy architecture to an abundance of new telephony products and services that inject calls and calling data from outside the control of the legacy telecommunications network. The telephony network then delivers to its destinations these calls and associated information, in most cases, without checking their validity. Consequently, this system supplies an opening for criminals to easily place calls with fabricated or "spoofed" ANIs for nefarious purposes. ANI fabrication or spoofing is a low cost, powerful penetration tool used to impersonate identity and location. Multiple companies and, more importantly, technologies exist for the sole purpose of enabling anyone, anywhere, to spoof ANI and Caller ID for pennies each call.

Throughout the past 25 years, telecommunication users have relied on ANI and have built vital business processes around the incoming calling party telephone number. In addition, most businesses have developed sophisticated inbound telephone answering systems (known as, for example, integrated voice response ("IVR") systems) that answer calls and are programmed with rules-based decision parameters grounded on the ANI information. Relying on non-validated ANI information undermines these critical marketing, technical, and security processes used for authentication, identity, location, customer service and activation in today's financial services, general business, and government enterprises. As one specific industry example, major financial institutions now have compromised critical operations that were built upon the trustworthiness of ANI. Applications such as bank-card activation, credit issuance, money transfers, new account applications, and customer service have all relied on the layer of security ANI has provided. Decisions made using the current non-validated ANI place an enterprise at risk of diminished revenue by limiting new product offerings and increased losses from fraud. Attempted fraud is estimated to exceed $50 billion each year in the U.S. alone. Identity fraud is a key driver in these losses. Today, bank card activation fraud occurs by telephone as frequently as other remote banking channels (i.e., not face-to-face), such as ATM, email, and world wide web.

There are several ways in which a motivated individual can take advantage of the current state of the art to manipulate ANI. VoiceXML applications let users change ANI and Caller ID information. An open source PBX software application, such as Asterisk, allows users to manipulate ANI information. Competitive service providers and telecommunication carriers can set their own ANI information. Moreover, certain companies exist today for the sole purpose of allowing ANI and Caller ID to be spoofed and falsified. Businesses such as PhoneGangster, Telespoof, CovertCall, and dozens of others offer widely available ANI and Caller ID spoofing for pennies each call.

The consequences of prevalent, facile manipulation of ANI and caller ID information provide motivation to restore integrity to the use of ANI and caller ID. One major consequence of falsified ANI and caller ID information is financial fraud, which is on the rise and is driven primarily by identity fraud. Traditional financial services customer verification tools such as information-based authentication are being compromised. Most financial service companies use ANI as the apex identifier in their telephonic decision-making. If false trust is placed in spoofed ANI, downstream decisions are compromised. Decisions made using current non-validated ANI is placing companies at risk, limiting new product offerings, and increasing losses from fraud. The disclosed approach restores the value of ANI and thereby helps to reestablish the security of telephone transactions.

There are as many financial transactions conducted over the telephone as are conducted on the world wide web, even in today's Internet pervasive environment. Of the more than nine billion telephone calls placed annually to U.S. financial institutions alone, nearly all rely on ANI for security, location information, call routing, and identity authentication. Knowing the caller's location or that the caller is in possession of an actual telephonic device is the foundation and an important factor for trusted telephone commerce.

The industry and legislators have grappled for many years to combat ANI and caller ID spoofing. In 2003, VoiceXML applications let users change ANI, and, at the same time, VoIP telephony entered the marketplace. An open source PBX software application, called Asterisk, allows users to manipulate calling party number information. Asterisk is a software implementation of a telephone private branch exchange (PBX) originally created in 1999 by Mark Spencer of Digium. As an example, if the ANI field is left blank by the Asterisk or carrier switch, any user can easily manipulate the Caller ID information using Asterisk, thereby populating the ANI field with the same misinformation as the spoofed Caller ID. Asterisk allows users to send spoofed ANI in the same way that businesses had been setting their ANI with PRI lines.

In 2004, a new ANI spoofing service, named Star38, (using VoIP and Asterisk) was launched and gained attention from worldwide mainstream media after USA Today published in its daily paper a front-page article about the service. The same year, others followed such as Camophone, Telespoof, and CovertCall. Over the next year, a dozen additional services started delivering ANI spoofing services.

By 2006, the FCC began investigations into these services, and the House of Representatives and the Senate considered several bills attempting to outlaw use of ANI spoofing for fraudulent purposes. ANI spoofing gained the attention of the mainstream media as SpoofCard announced the cancellation of an account belonging to Paris Hilton that was used to break into the voicemail of Lindsay Lohan to harass her.

On Jun. 27, 2007, the United States Senate Committee on Commerce, Science and Transportation approved and submitted to the Senate calendar Senate Bill 5.704, which would have made spoofing ANI a crime. Titled the "Truth in Caller ID Act of 2007," the bill would have outlawed causing "any caller identification service to transmit misleading or inaccurate caller identification information" via "any telecommunications service or IP-enabled voice service." Law enforcement would have been exempted from the rule. A similar bill, HR251, was recently introduced and passed in the House of Representatives. It had been referred to the same Senate committee that approved 5.704. The bill never became law because the full Senate never voted on it; it was added to the Senate Legislative Calendar under General Orders, but no vote was taken, and the bill expired at the end of the 110th Congress. On Jan. 7, 2009, Senator Bill Nelson (FL) and three co sponsors reintroduced the bill as S.30, the Truth in Caller ID Act of 2009, which was the

bill referred to the same committee in the Senate. On Dec. 22, 2010, President Obama signed into law the Truth in Caller ID Act of 2009, which makes it unlawful for a person to transmit misleading or inaccurate caller ID information with an intent to defraud, it amends the Communications Act of 1934. Several of the States have passed bills making misleading Caller ID spoofing illegal.

What is needed are systems and methods to identify ANI and caller ID manipulation for determining trustworthiness of incoming calling party and billing number information.

BRIEF SUMMARY OF THE INVENTION

In an embodiment of the present invention, systems and methods for determining the trustworthiness of calling party information, such as caller ID and ANI information, contained in a call request are provided. In an embodiment, the method includes receiving a call request at a service provider network element, such as a telecommunication carrier switch. The call request includes, at least, a called telephone number and calling party information. A decision is made as to whether the call request should be verified by reviewing a database of called telephone numbers for monitoring. When the call request is to be verified, a determination is made whether a discrepancy exists between the calling party information contained within the call request and authenticated stored calling party information. For example, the caller ID information in a call request is compared to service provider caller ID information for the calling party to determine if they match. When a discrepancy exists, a discrepancy report is transmitted to the called party contained in the call request or its agent to alert them of a potential problem in the trustworthiness of the call information that they will receive through normal call processing of the call request.

Further embodiments, features, and advantages of the invention, as well as the structure and operation of the various embodiments of the invention are described in detail below with reference to accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated herein and form a part of the specification, illustrate the present invention and, together with the description, further serve to explain the principles of the invention and to enable a person skilled in the pertinent art to make and use the invention.

FIG. **1** is a diagram of calling party information verification system, according to an embodiment of the invention.

FIG. **2** is a simplified network diagram providing an exemplary illustration of calling party information verification system interfaced with a telecommunications network, according to an embodiment of the invention.

FIG. **3** provides a flow chart of a method to verify a call request, according to an embodiment of the invention.

FIG. **4** is a diagram of a computer system on which the methods and systems herein described can be implemented, according to an embodiment of the invention.

The present invention will now be described with reference to the accompanying drawings. In the drawings, like reference numbers can indicate identical or functionally similar elements. Additionally, the left-most digit(s) of a reference number may identify the drawing in which the reference number first appears.

DETAILED DESCRIPTION OF THE INVENTION

As discussed above spoofing or falsifying of ANI or caller ID information has potentially significant negative impacts to various types of services, such as credit card activations, that rely on the authenticity of ANI and caller ID information. The present invention addresses the problems highlighted above, by providing systems and methods of identifying and reporting discrepancies to calling party information, such as ANI and caller ID information.

When discrepancies exist, the discrepancies are reported to the called party, an agent of the called party or another third party for consideration and analysis to help identify and potentially reduce fraudulent activities. In particular, ANI and Caller ID discrepancy reporting can assist in the determination of the trustworthiness and credibility of calling party number identification. Embodiments of the invention entail the use of real time telephone switch signaling messages, network data, stored data of switch telephone numbers and Direct Inbound Dialing (DID) numbers (also referred to as extensions) and lists of phone numbers monitored for discrepancy detection and reporting. In embodiments, practice of the disclosed methods is neither detectable by caller nor by called party. Embodiments of the invention can be implemented within existing telecommunication infrastructure. Importantly, in embodiments of the invention, given various privacy concerns and Federal Communications Commission rules, customer proprietary network information (CPNI) is not made available to third parties. In these embodiments, the discrepancy reports received by the called party, third party agent, or any other party do not include the originating number or any other CPNI information. In embodiments, where authorized (e.g., by a police or FBI warrant) discrepancy reports include CPNI information.

FIG. **1** provides a diagram of calling party information verification system **100** according to an embodiment of the invention. Calling party verification system **100** includes service provider interface **110**, discrepancy detector **120**, network interface **130**, monitored called party number database **140**, and service provider assigned calling party information database **150**. In an embodiment, the operation of calling party verification system **100** is not detectable by the calling party or the called party, as shown in FIG. **2**.

FIG. **2** provides a simplified network diagram providing an exemplary illustration of calling party information verification system **100** interfaced with a telecommunications network, according to an embodiment of the invention. The description of calling party verification system **100** is provided relative to the simplified network diagram for illustration purposes only, and is not intended to limit the scope of the invention to the simplified network. The simplified network diagram portion of FIG. **2**, provides calling party device **210**, service provider network element **220**, communication network **230**, and called party device **240**. Calling party device **210** and called party device **240** can be any type of device used to place or receive a telephone call, such as, but not limited to an analog telephone, a digital telephone, a wireless telephone, a computer telephony device, a VOIP-based telephone, or a private branch exchange (PBX) supporting multiple lines or key system supporting multiple lines. Service provider network element **220** includes, but is not limited to, analog switches (e.g., 1AESS), digital switches (e.g., 5ESS), IP network switches, and IP network routers. Communications network **230** includes, but is not limited to wireline and wireless networks, traditional plain

old telephone service (POTS) networks, IP-based networks and any combination of these types of networks.

Calling party device **210** transmits a call request containing calling party information, as well as called party information (e.g., the telephone number of called party device **240**). Upon receipt of the call request, service provider network element **220** processes the call and provides further signaling to communications network **230** in order to complete the call to called party device **240**. Calling party verification system **100** is interfaced with service provider network element **220** to verify the calling party information contained within the call request.

Calling party verification system **100** may be interfaced to service provider network element in a variety of ways. Aspects of calling party verification system **100** may be integrated within the software of service provider network element **220** or calling party verification system **100** may be coupled to service provider network element **220** as an adjunct to the element. Further, as shown in FIG. **2**, calling party verification system **100** is coupled to Internet **250**, which in turn is coupled to called party agent **260**. In embodiments Internet **250** may alternatively be a virtual private network, private network or other form of computer network that supports transmission of messages from calling party verification system **100** to called party agent **260**.

Referring to FIG. **1**, service provider interface **110** is configured to receive call request information from a service provider network element, such as service provider network element **220**, which receives a call request having calling party information to a called telephone number. For example, calling party device **210** generates a call request. The call request includes calling party information about calling party device **210** and includes called party information about called party device **240** that is used to route the call properly. In an embodiment, service provider interface **110** also provides a pathway between discrepancy detector **120** and service provider network element to enable discrepancy detector **120** to log the discrepancy, and/or to halt call processing of a call associated with a call request that generates a discrepancy.

In embodiments, calling party information is ANI information, caller ID information or both. Additionally, the call request can be received using various network protocols, including, but not limited to Session Initiation Protocol (SIP), Integrated Services Digital Network (ISDN), Plain Old Telephone Service (POTS), Time Division Mulitplexing (TDM) or Voice over Internet Protocol (VOIP) call messaging protocols.

Discrepancy detector **120** is coupled to service provider interface **210**, and is configured to determine whether a discrepancy exists between the calling party information contained within the call request and stored calling party information. Specifically, discrepancy detector **120** is configured to determine whether the call request to the called telephone number is to be verified and determine whether a discrepancy exists between calling party information contained within the call request and stored calling party information when the call request is to be verified. In an embodiment, in order to determine whether a call request is to be verified, discrepancy detector will access monitored called party number database **140**. If the called party number matches a number in the monitored called party number database, discrepancy detector **120** will verify the calling party information in the call request.

Discrepancy detector **120** generates a discrepancy report when a discrepancy exists between calling party information contained within the call request and stored calling party information. In an embodiment, a discrepancy exists when the calling party information in the received call request does not match calling party information stored within service provider assigned calling party information database **150** for the calling party. For example, if the ANI or caller ID information in the call request does not match the ANI or caller ID information that is stored in service provider assigned calling party information database **150**, a discrepancy is generated.

In another embodiment, discrepancy detector **120** initiates a look-up in an external database other than service provider assigned calling party information database **150** to support discrepancy analysis. For example, discrepancy detector **120** launches a query to a local number portability database to determine what service provider is assigned the ANI and/or caller ID information within the call request. If the service provider is a carrier, other than the carrier maintaining service provider network element **220**, then a discrepancy is determined to exist. In an alternative embodiment, called party agent **260** upon receipt of a discrepancy report can conduct additional analysis of the discrepancy report, including, but not limited to, querying a local number portability database to determine what service provider is assigned the ANI and/or caller ID information within the call request.

Discrepancy detector **120** captures call parameters associated with the call request, when a discrepancy exists. Call parameters include one or more of an identity of the service provider receiving the call request, the caller ID and/or ANI information, the called party number, a type of discrepancy event, a date of the call request, and/or a time of the call request, preferably in GMT. As an example, a type of discrepancy event is that caller ID information in the call request did not match caller ID information in service provider assigned calling party information database **150**.

Network interface **130** is coupled to discrepancy detector **120**, and transmits discrepancy reports. Network interface **130** transmits the discrepancy reports to the called party or an agent for the called party, such as called party agent **260**. Network interface **130** also can transmit a discrepancy report prior to further processing of a call requested in the call request, transmit the discrepancy report during processing of a call requested in the call request and before call completion to the called party, or transmit the discrepancy report after call completion to the called party. If the discrepancy report is transmitted after call completion, the report can be transmitted either individually or in a batch transmission with other discrepancy reports.

Monitored called party number database **140** is coupled to the discrepancy detector, and contains telephone numbers for called party numbers for which call request validity is to be assessed. In an embodiment, monitored called party number database **140** can be populated with toll free numbers and non-toll free numbers associated with a financial institutions credit card verification services. In another embodiment, called party number database **140** can be configured with an NPA-NXX, such that any individual number within that NPA-NXX block of telephone numbers will be monitored.

Service provider assigned calling party information database **150** is coupled to discrepancy detector **150**, and contains service provider assigned calling party information. Information, for example, may include mappings of caller ID and ANI information to the lines (e.g., POTS lines or VOIP extensions) upon which a call request is received.

FIG. **3** provides method **300** for verify a call request, according to an embodiment of the invention. In embodiments, method **300** is not detectable by the calling party, the called party, or both. Method **300** begins in step **310**. In step **310** a call request is received. The call request includes at least a called telephone number and calling party information. The calling party information can include, but is not limited to ANI information and/or caller ID information. Referring to FIG. **2**, for example, service provider network element **220** receives a call request, which is then received by discrepancy detector **120** via service provider interface **110**. In embodiments, the calling party information in the call request includes the ANI information of calling party device **210**. Alternatively, the calling party information in the call request includes caller ID information of calling party device **210**. And finally in another embodiment, the calling party information includes both the caller ID information and the ANI information of calling party device **210**. The call request will also include the telephone number of the called party, such as the telephone number of called party device **240**.

In step **320** a decision is made whether to verify the call request. When a call request is received, for example, discrepancy detector **120** compares the calling party number in the call request to telephone numbers stored in monitored called party number database **140**. If the calling party number in the call request matches a stored telephone number then the call request will be verified. Otherwise, the call request is not verified and method **300** proceeds to step **370** and ends. In this case, call processing proceeds as normal to complete the call to the called party. When a decision to verify the call request is made, method **300** proceeds to step **330**.

In step **330**, a discrepancy test on the calling party information contained in the call request is conducted. A variety of discrepancy tests can be conducted. In an embodiment, a discrepancy exists when calling party information received in a call request does not match stored calling party information assigned by a service provider receiving the call request, such as telephone number information stored in service provider assigned calling party information database **150**. For example, if the ANI information in the call request does not match ANI information for the calling party stored in service provider assigned calling party information database, then a discrepancy is determined to exist. In another example, if the caller ID information in the call request does not match caller ID information for the calling party stored in service provider assigned calling party information database, then a discrepancy is determined to exist

In step **340** a determination is made whether a discrepancy exists. If no discrepancy exists, method **300** proceeds to step **370** and call processing proceeds as normal to complete the call to the called party. If a discrepancy exists, method **340** proceeds to step **350**.

In step **350** a discrepancy report is generated. When a discrepancy report is generated, discrepancy detector **120** captures call parameters from the call request including one or more of an identity of the service provider receiving the call request, the called party number, the ANI and/or caller ID information of the call request, a type of discrepancy event, a date of the call request, and/or a time of the call request. These call parameters are added to the discrepancy report.

In step **360** the discrepancy report is transmitted. In embodiments, the discrepancy report is transmitted to the called party, an agent for the called party or another third party. In embodiments, transmitting the discrepancy report occurs prior to further processing of a call requested in the call request, during processing of a call requested in the call request and before call completion to the called party, or occurs after call completion to the called party. When the discrepancy report is transmitted after call completion, the discrepancy report is transmitted either individually or in a batch transmission with other discrepancy reports. The discrepancy report is transmitted via the Internet, virtual private network, or other type of network. In an optional step, when a discrepancy is detected, call processing of the call requested can be suspended or terminated, or the discrepancy event can be logged. For example, discrepancy detector **120** can cause a signal to be transmitted to service provider network element **220** to halt call processing.

In step **370** method **300** ends.

Computer System Implementation

Calling party verification system **100** can be implemented in hardware, software or a combination thereof. To the extent that software is used that software can be implemented and supported on a computer system, such as computer system **400**, as illustrated in FIG. **4**. Computer **400** includes one or more processors (also called central processing units, or CPUs), such as processor **410**. Processor **410** is connected to communication bus **420**. Computer **400** also includes a main or primary memory **430**, preferably random access memory (RAM). Primary memory **430** has stored therein control logic (computer software), and data.

Computer **400** may also include one or more secondary storage devices **440**. Secondary storage devices **440** include, for example, hard disk drive **450** and/or removable storage device or drive **460**. Removable storage drive **460** represents a magnetic tape drive, a compact disk drive, an optical storage device, tape backup, solid state drive, etc.

Removable storage drive **460** interacts with removable storage unit **470**. As will be appreciated, removable storage unit **460** includes a computer usable or readable storage medium having stored therein computer software (control logic) and/or data. Removable storage drive **460** reads from and/or writes to the removable storage unit **470** in a well known manner.

Removable storage unit **470**, also called a program storage device or a computer program product, represents a floppy disk, magnetic tape, compact disk, optical storage disk, or any other computer data storage device. Program storage devices or computer program products also include any device in which computer programs can be stored, such as hard drives, ROM or memory cards, etc.

In an embodiment, the present invention is directed to computer program products or program storage devices having software that enables computer **400**, or multiple computer **400**s to perform any combination of the functions described herein. Computer programs (also called computer control logic) are stored in main memory **430** and/or the secondary storage devices **440**. Such computer programs, when executed, direct computer **400** to perform the functions of the present invention as discussed herein. In particular, the computer programs, when executed, enable processor **410** to perform the functions of the present invention. Accordingly, such computer programs represent controllers of the computer **400**.

Computer **400** also includes input/output/display devices **480**, such as monitors, keyboards, pointing devices, etc. Computer **400** further includes a communication or network interface **490**. Network interface **490** enables computer **400** to communicate with remote devices. For example, network interface **490** allows computer **400** to communicate over communication networks, such as LANs, WANs, the Internet, etc. Network interface **490** may interface with remote sites or networks via wired or wireless connections. Computer **400** receives data and/or computer programs via network interface **490**.

CONCLUSIONS

The invention can work with software, hardware, and operating system implementations other than those described herein. Any software, hardware, and operating system implementations suitable for performing the functions described herein can be used.

The present invention has been described above with the aid of functional building blocks illustrating the implementation of specified functions and relationships thereof. The boundaries of these functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternate boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed.

The foregoing description of the specific embodiments will so fully reveal the general nature of the invention that others can, by applying knowledge within the skill of the art, readily modify and/or adapt for various applications such specific embodiments, without undue experimentation, without departing from the general concept of the present invention. Therefore, such adaptations and modifications are intended to be within the meaning and range of equivalents of the disclosed embodiments, based on the teaching and guidance presented herein. It is to be understood that the phraseology or terminology herein is for the purpose of description and not of limitation, such that the terminology or phraseology of the present specification is to be interpreted by the skilled artisan in light of the teachings and guidance.

What is claimed is:

1. A computer-implemented method, comprising:

receiving from a calling party by a discrepancy detector a call request having a called telephone number, wherein the call request includes calling party information, wherein the discrepancy detector determines discrepancies in calling party information and is ancillary to an originating service provider network element that provides a telephone line for the calling party placing the call request;

accessing a monitored called party number database, wherein accessing the monitored called party number database includes determining whether the call request to the called telephone number is to be verified, wherein the monitored called party number database includes telephone numbers;

when the call request is to be verified, determining by the discrepancy detector whether a discrepancy exists between the calling party information contained within the call request and stored calling party information; and

when a discrepancy exists between the calling party information contained within the call request and stored calling party information, causing call processing of a call requested in the call request to be suspended.

2. The method of claim **1**, further comprising when a discrepancy exists between the calling party information contained within the call request and stored calling party information, generating a discrepancy report.

3. The method of claim **2**, further comprising capturing call parameters from the call request.

4. The method of claim **3**, wherein the call parameters include one or more of an identity of the originating service provider receiving the call request, Automatic Number Identification information from the call request, caller identification (caller ID) information from the call request, the called party number, a type of discrepancy event, a date of the call request, and/or a time of the call request.

5. The method of claim **2**, further comprising transmitting the discrepancy report to a called party or an agent for the called party.

6. The method of claim **5**, wherein transmitting the discrepancy report occurs prior to further processing of a call requested in the call request.

7. The method of claim **5**, wherein transmitting the discrepancy report occurs during processing of a call requested in the call request and before call completion to the called party.

8. The method of claim **5**, wherein transmitting the discrepancy report occurs after call completion to the called party, wherein the discrepancy report is transmitted either individually or in a batch transmission with other discrepancy reports.

9. The method of claim **5**, wherein transmitting the discrepancy report comprises transmitting the discrepancy report via the Internet or a virtual private network.

10. The method of claim **2**, further comprising causing call processing to be terminated.

11. The method of claim **1**, wherein a discrepancy exists when calling party info nation received in a call request does not match stored calling party information assigned by a service provider receiving the call request.

12. The method of claim **1**, wherein calling party information includes Automatic Number Identification information or caller identification (caller ID) information.

13. The method of claim **1**, wherein the calling party information is included in a Session Initiation Protocol, Integrated Services Digital Network, Plain Old Telephone Service, Time Division Multiplexing, or Voice over Internet Protocol call set up message.

14. The method of claim **1**, wherein detecting a discrepancy within the call request is not detectable by the calling party.

15. A computer-implemented method, comprising:

receiving from a calling party by a discrepancy detector a call request having a called telephone number, wherein the call request includes calling party information, wherein the discrepancy detector determines discrepancies in calling party information and is ancillary to an originating service provider network element that provides a telephone line for the calling party placing the call request;

accessing a monitored called party number database, wherein accessing the monitored called party number database includes determining whether the call request to the called telephone number is to be verified, wherein the monitored called party number database includes telephone numbers, wherein the telephone numbers include only telephone numbers and related information for called party numbers for which call request validity is to be assessed;

when the call request is to be verified, determining by the discrepancy detector whether a discrepancy exists between the calling party information contained within the call request and stored calling party information.

16. The method of claim **15**, further comprising when a discrepancy exists between the calling party information contained within the call request and stored calling party information, generating a discrepancy report.

17. The method of claim **16**, further comprising capturing call parameters from the call request.

18. The method of claim **17**, wherein the call parameters include one or more of an identity of the originating service provider receiving the call request, Automatic Number Identification information from the call request, caller identification (caller ID) information from the call request, the called party number, a type of discrepancy event, a date of the call request, and/or a time of the call request.

19. The method of claim **16**, further comprising transmitting the discrepancy report to a called party or an agent for the called party.

20. The method of claim **19**, wherein transmitting the discrepancy report occurs prior to further processing of a call requested in the call request.

* * * * *

Exhibit 4

US009762728B1

(12) United States Patent
Cox et al.

(10) Patent No.: **US 9,762,728 B1**
(45) Date of Patent: **Sep. 12, 2017**

(54) **USING CALLING PARTY NUMBER FOR CALLER AUTHENTICATION**

(71) Applicant: **TrustID, Inc.**, Lake Oswego, OR (US)

(72) Inventors: **Patrick Michael Cox**, Newberg, OR (US); **Shreyas Dattatraya Saitawdekar**, Portland, OR (US); **Richard J. Greene**, Portland, OR (US); **Daniel V. Stone**, Portland, OR (US)

(73) Assignee: **TrustID, Inc.**, Lake Oswego, OR (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **15/367,749**

(22) Filed: **Dec. 2, 2016**

(51) **Int. Cl.**

H04M 1/56	(2006.01)
H04M 15/06	(2006.01)
H04M 3/38	(2006.01)
H04W 12/06	(2009.01)
H04M 3/42	(2006.01)

(52) **U.S. Cl.**
CPC ***H04M 3/382*** (2013.01); ***H04M 3/42042*** (2013.01); ***H04W 12/06*** (2013.01)

(58) **Field of Classification Search**
CPC ... H04L 2209/56; H04L 63/08; H04L 3/0876; H04M 3/42059; H04M 3/436; H04M 3/54; H04M 2203/6027; H04M 2203/6045; G06F 2221/2101; G06F 2221/2117; G06F 21/42; G06F 21/23; G06F 21/44; G06F 2221/2123; G06Q 20/32; G06Q 20/42; G06Q 30/04; G06Q 30/0601; G06Q 40/025
USPC 379/100.03, 100.05, 100.06, 100.12, 379/102.02, 102.07, 142.01, 142.04, 379/142.05, 142.1, 142.17
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,822,703	B1 *	10/2010	Rodriguez-Val	G06F 21/42 705/26.1
8,520,832	B1 *	8/2013	Condreay	H04M 3/42059 379/265.12
9,197,746	B2 *	11/2015	Kurapati	H04L 63/126
9,332,119	B1 *	5/2016	Danis	H04M 3/42042
2006/0233160	A1 *	10/2006	Kawanishi	H04L 29/06027 370/352

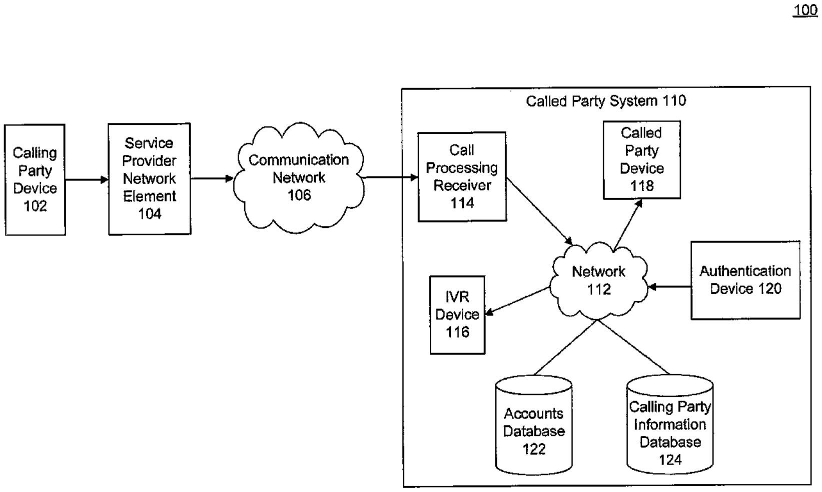
(Continued)

Primary Examiner — Binh Tieu
(74) *Attorney, Agent, or Firm* — Sterne, Kessler, Goldstein & Fox P.L.L.C.

(57) **ABSTRACT**

Embodiments include a system, method, and computer program product that authenticates a caller using calling party information. In an embodiment, an authentication device receives the call request and associated calling party information that includes a calling party number. The authentication device retrieves parameters associated with the calling party number, where a retrieved parameter is a number of accounts linked to the calling party number. The authentication device determines whether the number of accounts is between one and a threshold value, inclusive, and verifies that the call request originates from a location or a device associated with the calling party number. Based on the verifying and determining, the authentication device generates an authentication result that indicates whether the calling party number is authenticated. Then, the authentication device sends the authentication result to a call processing device that processes the call request from the caller according to the authentication result.

20 Claims, 6 Drawing Sheets


100
Calling Party Device 102
Service Provider Network Element 104
Communication Network 106
Called Party System 110
Call Processing Receiver 114
Called Party Device 118
Network 112
Authentication Device 120
IVR Device 116
Accounts Database 122
Calling Party Information Database 124

(56) **References Cited**

U.S. PATENT DOCUMENTS

2011/0185406	A1 *	7/2011	Hirson	G06Q 20/32 726/6
2012/0295580	A1 *	11/2012	Corner	H04W 12/12 455/405
2016/0226872	A1 *	8/2016	Oberheide	G06F 21/44

* cited by examiner

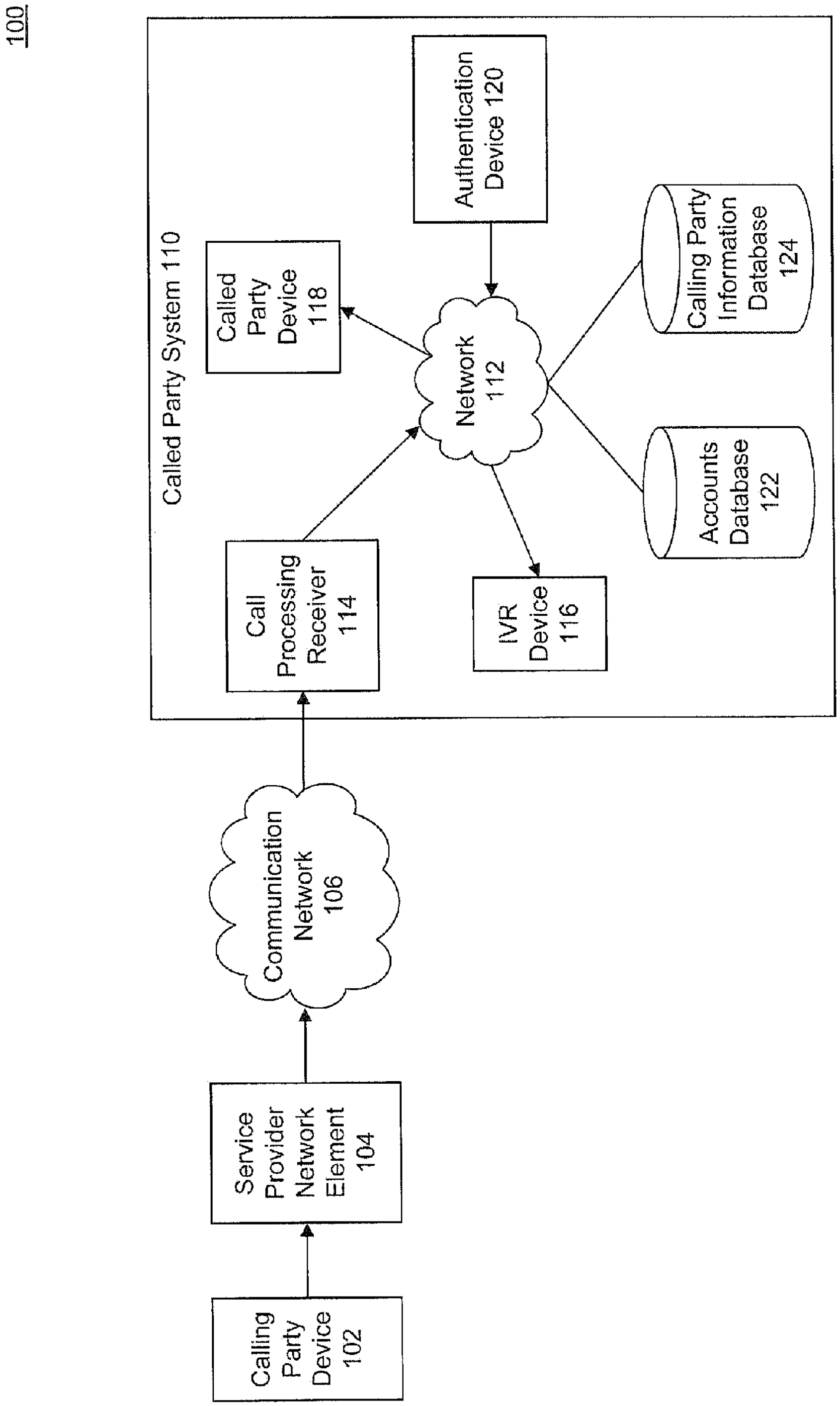

100
Called Party System 110
Authentication Device 120
Called Party Device 118
Network 112
Calling Party Information Database 124
Accounts Database 122
Call Processing Receiver 114
IVR Device 116
Communication Network 106
Service Provider Network Element 104
Calling Party Device 102

FIG. 1

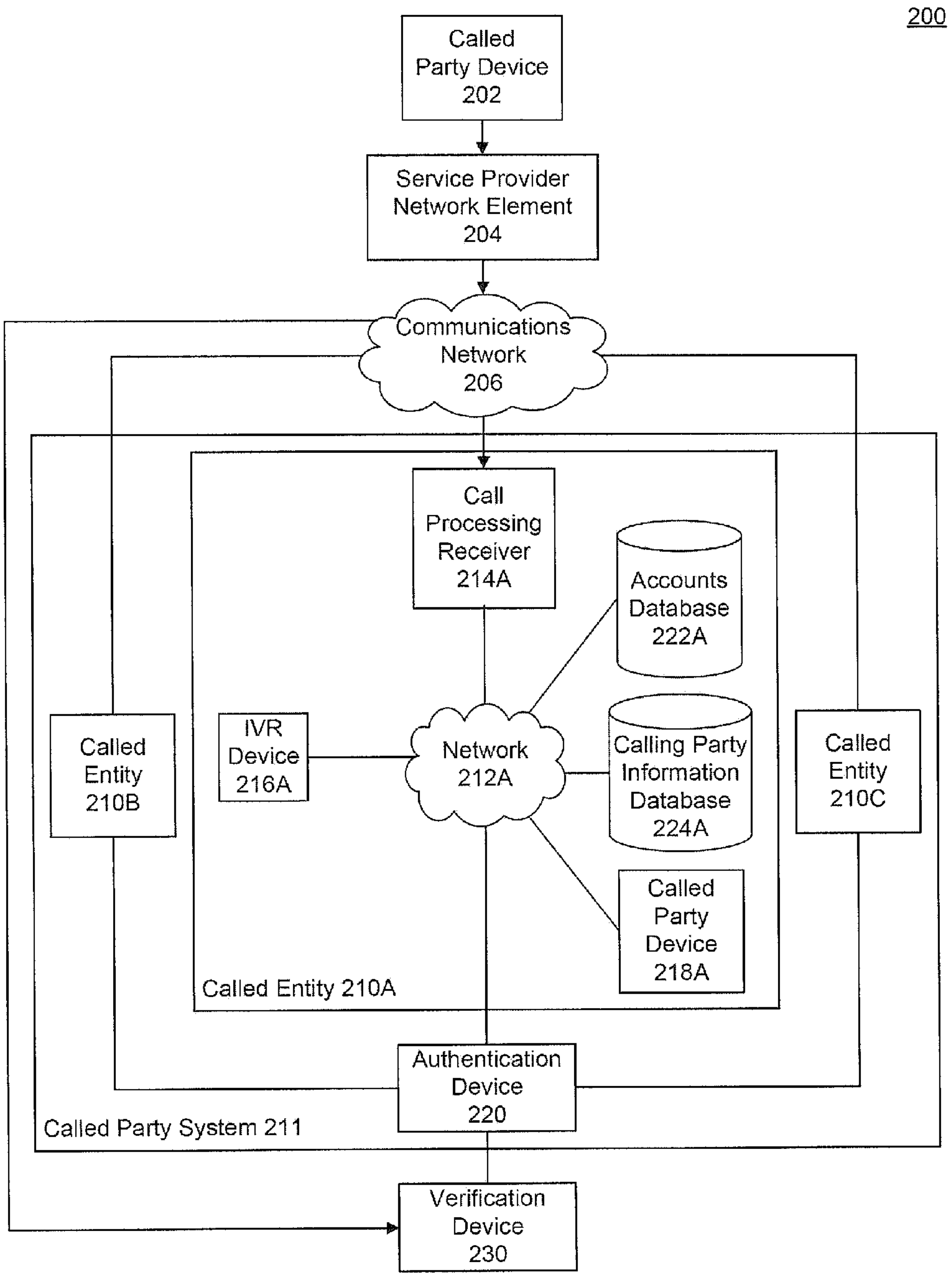

200
Called Party Device 202
Service Provider Network Element 204
Communications Network 206
Call Processing Receiver 214A
Accounts Database 222A
IVR Device 216A
Network 212A
Calling Party Information Database 224A
Called Party Device 218A
Called Entity 210A
Called Entity 210B
Called Entity 210C
Authentication Device 220
Called Party System 211
Verification Device 230

FIG. 2

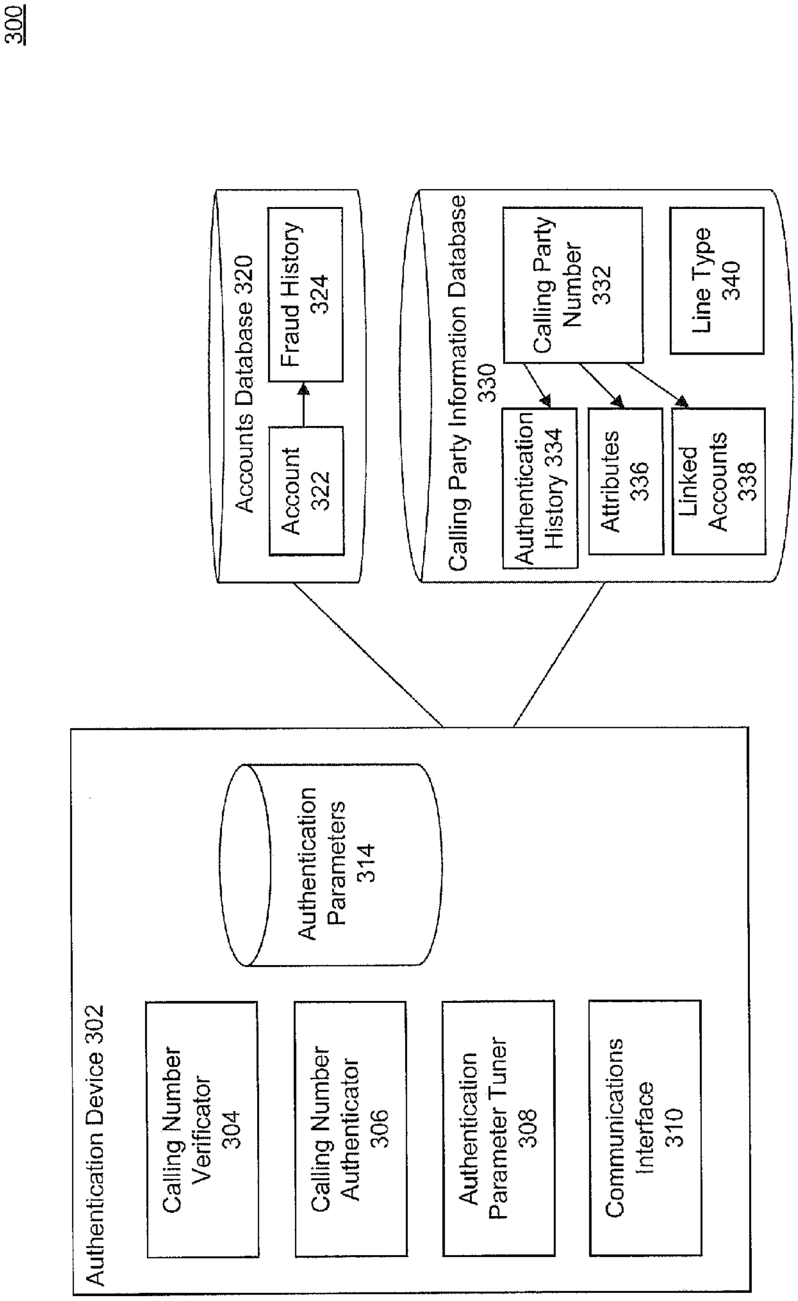

300
Accounts Database 320
Account 322
Fraud History 324
Calling Party Information Database 330
Calling Party Number 332
Authentication History 334
Attributes 336
Linked Accounts 338
Line Type 340
Authentication Device 302
Calling Number Verificator 304
Calling Number Authenticator 306
Authentication Parameter Tuner 308
Communications Interface 310
Authentication Parameters 314

FIG. 3

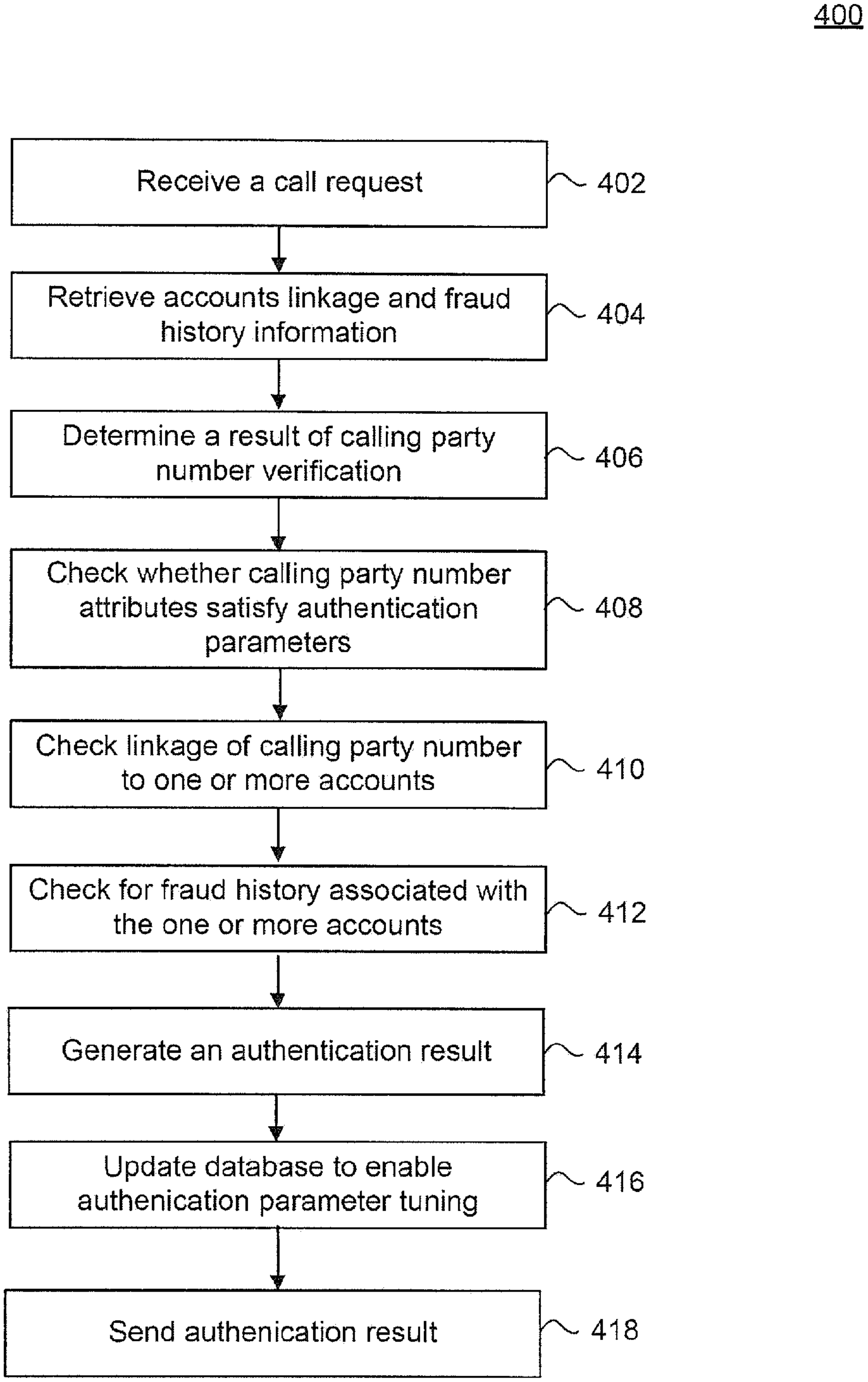

400
Receive a call request
402
Retrieve accounts linkage and fraud history information
404
Determine a result of calling party number verification
406
Check whether calling party number attributes satisfy authentication parameters
408
Check linkage of calling party number to one or more accounts
410
Check for fraud history associated with the one or more accounts
412
Generate an authentication result
414
Update database to enable authenication parameter tuning
416
Send authenication result
418

FIG. 4

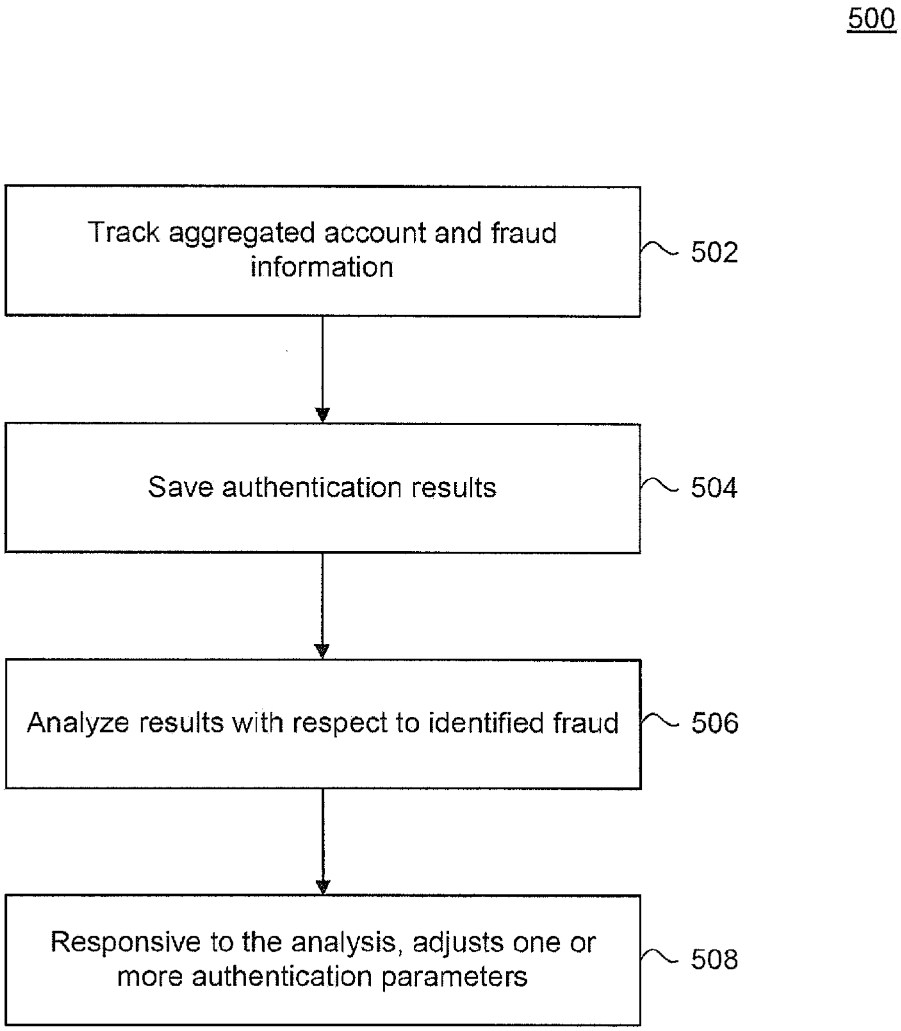

500
Track aggregated account and fraud information
502
Save authentication results
504
Analyze results with respect to identified fraud
506
Responsive to the analysis, adjusts one or more authentication parameters
508

FIG. 5

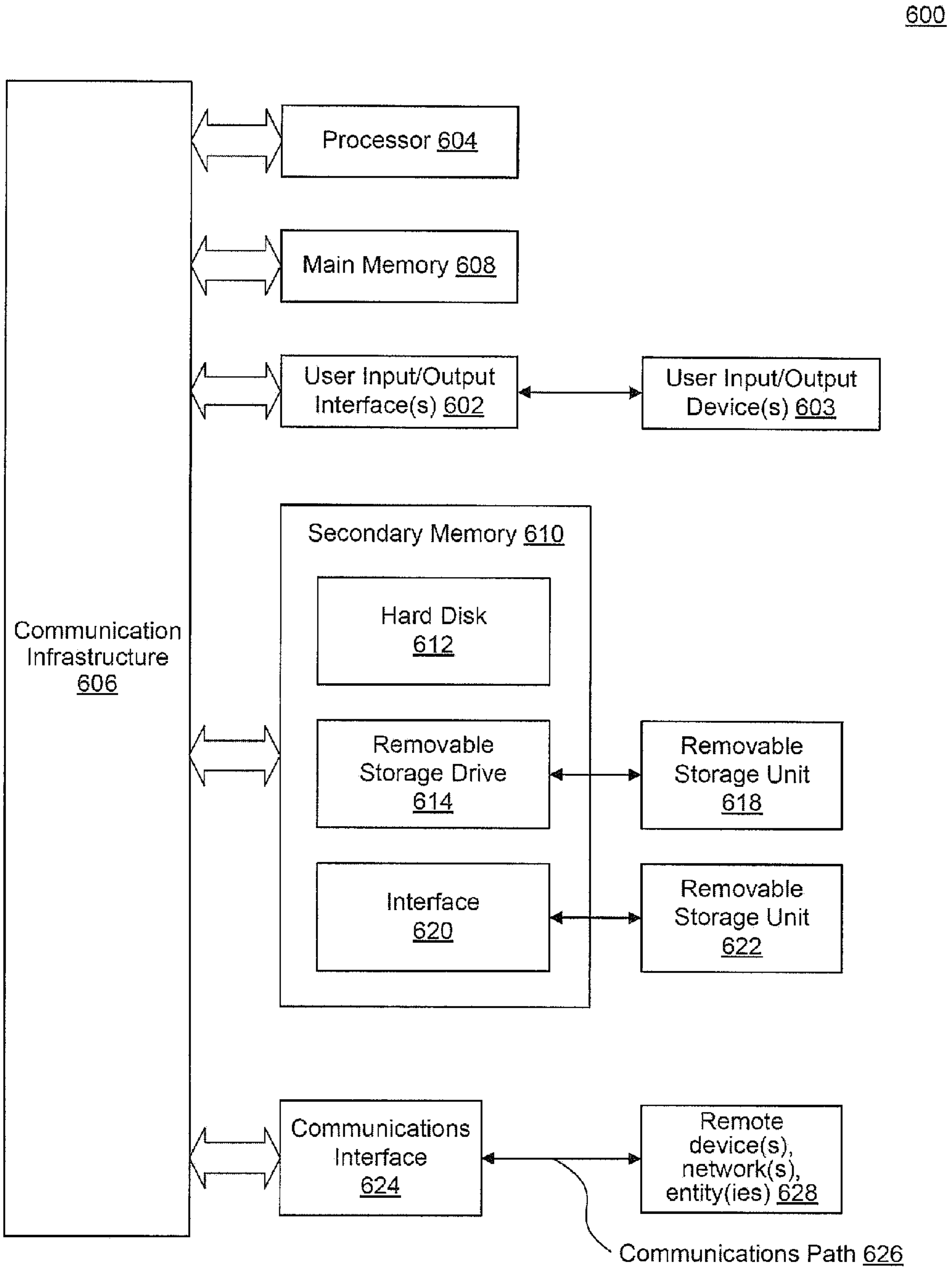

600
Processor 604
Main Memory 608
User Input/Output Interface(s) 602
User Input/Output Device(s) 603
Secondary Memory 610
Hard Disk 612
Removable Storage Drive 614
Removable Storage Unit 618
Interface 620
Removable Storage Unit 622
Communication Infrastructure 606
Communications Interface 624
Remote device(s), network(s), entity(ies) 628
Communications Path 626

FIG. 6

USING CALLING PARTY NUMBER FOR CALLER AUTHENTICATION

BACKGROUND

Copyright Notice

Field of the Invention

The embodiments relate generally to calls placed in telecommunication and information service networks.

Related Art

Automatic Number Identification (ANI) is a service that provides to the recipient of the call the call's class of service and a 10-digit billing telephone number of a caller. Introduced in the 1960s, ANI informed business telephone customers with toll free circuits (800 or "Inward-WATS") who was calling, because the called business was paying tolls for the incoming call. Later, ANI and Calling Number Identification (Caller ID) were available to customers without toll free circuits to provide them with the 10-digit telephone number of the calling party. By the late 1980s, calling name services provided a caller's name, in addition to the caller's 10-digit number and class of service.

Businesses such as banks, call centers, and government entities, such as 911 service centers, have used ANI information to determine identity and to discover location. ANI information is also used for call routing assistance, workflow efficiency, authentication, and fraud mitigation. In one example, some businesses have inbound telephone answering systems (known as, for example, integrated voice response ("IVR") systems) that answer calls and are programmed with rules-based decision parameters based on the ANI information. Major financial institutions rely on ANI for bank-card activation, credit issuance, money transfers, new account applications, and customer service. These major financial institutions have relied on the layer of security that ANI provides.

Ways to control or manipulate ANI and caller ID information, however, are available. Historically, only telecommunications carriers and very large business users who subscribed to expensive multi-line Primary Rate Interface telephone circuits had the ability to manipulate ANI. For example, a large business may control ANI to display its main telephone number on all outgoing calls from its multiple lines, rather than each of the individual lines.

More recently, ANI and caller ID information has become easier to manipulate. Before the advent of information services network (e.g., Internet) telephony and deregulation, the telecommunications network was a closed system with one or both of a limited number of trusted FCC- and Public Utility Commission-licensed telecommunications companies adhering to a finite set of standards. Telecommunications decentralization and deregulation, as well as Internet telephony (e.g., Voice over Internet Protocol (VoIP) technology), have exposed this legacy architecture to new telephony products and services that inject calls and calling data from outside the legacy telecommunications network. The telephony network then delivers these calls and associated information, in most cases, without checking the ANI information's validity.

Because ANI and caller ID information can be more easily manipulated, individuals can more easily place calls with fabricated or "spoofed" ANIs for nefarious purposes. ANI fabrication or spoofing is a low cost, powerful penetration tool used to impersonate identity and location. VoiceXML applications let users change ANT and Caller ID information. Open source PBX software applications, such as Asterisk and FreeSwitch, allow users to manipulate ANI information. As an example, if the ANT field is left blank by the Asterisk or carrier switch, any user can easily manipulate the Caller ID information using Asterisk, thereby populating the ANI field with the same misinformation as the spoofed Caller ID. Asterisk allows users to send spoofed ANI in much the same way that businesses had been setting their ANI with PRI lines. Competitive service providers and telecommunication carriers can set their own ANI information. Multiple companies exist for the sole purpose of enabling anyone, anywhere, to spoof ANI and Caller ID for pennies each call.

Relying on inaccurate ANI information can undermine marketing, technical, and security processes used for authentication, identity, location, customer service, and activation. Decisions made using the current non-validated ANI place an enterprise at risk of diminished revenue by limiting new product offerings, increasing operational costs, and increasing losses from fraud.

Of the more than ten billion telephone calls placed annually to U.S. financial institutions alone, nearly all rely on ANI for security, location information, call routing, and identity authentication. For example, bank card activation fraud occurs by telephone as frequently as other remote banking channels (i.e., not face-to-face), such as ATM, email, and the World Wide Web. Knowing the caller's location or that the caller is in possession of an actual telephonic device is the foundation and an important factor for trusted telephone commerce.

On Dec. 22, 2010, President Obama signed into law the Truth in Caller ID Act of 2009, which makes it unlawful for a person to transmit misleading or inaccurate caller ID information with an intent to defraud; the Act amends the Communications Act of 1934. Several of the States have passed bills making misleading Caller ID spoofing illegal.

The Truth in Caller ID Act of 2009, however, does not itself guarantee that ANI can be trusted as is. Consequently, banks and other businesses often require additional factors of authentication to confirm the identity of a calling party. For example, IVRs or agents at call centers may require a calling party to input personally identifiable information (PII) to confirm the caller's identity. PII may include, for example, a social security number or a date of birth. Requesting additional PII information may prolong calls and further increase the processing time and resources of IVRs or agents.

Moreover, using PII to conduct information-based authentication has many challenges and risks. For example, information-based authentication using PII such as social security numbers or a mother's maiden names exposes the bank to additional risk. PII information is regulated, and, if the PII information in the bank's possession is lost or stolen from the bank, large costs and fines can be levied against the bank by government entities enforcing current data breach laws.

Additionally, because of the high number of past data breaches, a very high percentage of consumers have had their PII data compromised already, making PII available to criminals for use in ID theft (In **2016**, the Identity Theft Resource Center reported 6,333 breaches and 864 million records exposed since 2005.) In addition, social networking websites such as Facebook, LinkedIn, Ancestry, Twitter, and dozens more make PII readily available for the public, further de-valuing the use of PII knowledge as a tool for identity authentication. ANI is one of the authentication tools available to banks and other businesses that are not PII-based for telephone-based transactions.

BRIEF SUMMARY OF THE INVENTION

What is needed are system, method, or computer program product embodiments, or combinations and sub-combinations thereof, for using calling party information to authenticate the calling party so that the calling party's call request can be processed more efficiently. In an embodiment, an authentication device receives the call request and associated calling party information, the calling party information including a calling party number. The authentication device retrieves parameters associated with the calling party number, where a retrieved parameter may include a number of accounts linked to the calling party number, a number of occurrences and associated dates of fraud on those linked accounts, a device or location type, a status of the network signaling, or a trustworthiness of the calling party number. In an embodiment, the authentication device determines whether the number of accounts is between one and a threshold value, inclusive. The authentication device also verifies that the call request originates from a valid and trustworthy location or from a device associated with the calling party number and linked to a valid account or a threshold number of accounts. Further, based on the verifying and whether the number of accounts is determined to be between one and a threshold value, the authentication device generates an authentication result indicating whether the calling party number is authenticated. An authenticated calling party number, associated with the call request, can then be used as an ownership token of authentication to authenticate the caller. In an embodiment, the authentication device further determines whether the one or more linked accounts is free of fraudulent activity between one day and a threshold value of days to generate the authentication result. Upon generating the authentication result, the authentication device sends the authentication result to a call processing device that processes the call request according to the authentication result.

Further embodiments, features, and advantages of the invention, as well as the structure and operation of the various embodiments of the invention are described in detail below with reference to accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS/FIGURES

The accompanying drawings are incorporated herein and constitute a part of this specification. In the drawings:

FIG. **1** is a block diagram of a system for call authentication based on calling party information, according to an embodiment.

FIG. **2** is a block diagram of distributed system for call authentication based on calling party information, according to an embodiment.

FIG. **3** is a block diagram of a system for authenticating a caller based on calling party information, according to an embodiment.

FIG. **4** is a flowchart of a method for generating an authentication result, according to an embodiment.

FIG. **5** is a flow chart of a method for improving accuracy of generating authentication results, according to an embodiment.

FIG. **6** is a diagram of a computer system on which the methods and systems herein described can be implemented, according to an embodiment.

In the drawings, like reference numbers generally indicate identical or similar elements. Additionally, generally, the left-most digit(s) of a reference number identifies the drawing in which the reference number first appears.

DETAILED DESCRIPTION

Currently, authenticating a caller that originated a call request entails requesting the caller to submit, either vocally or via keypad, caller personal identifying information. But, caller identifying information is not a reliable indicator for authenticating the caller and the call request because caller identifying information may be easily obtained by unauthorized callers. In contrast, embodiments are described herein that use calling party information to authenticate the calling party information to authorize the calling party's call request without prolonging the call and achieving a high rate of fraud detection. In an embodiment, an authentication device analyzes a calling party number, included in the calling party information, associated with a received call request. As part of this analysis, the authentication device retrieves parameters associated with the calling party number. These parameters may include the number of accounts linked to the calling party number. This analysis further includes verifying the call request based on the calling party number, and determining whether the number of accounts, associated with the calling party number, is between one and a threshold value, inclusive. In an embodiment, the analysis further includes determining occurrences and associated dates of fraud on linked accounts, a device or location type associated with the call request, a status, validity, and truthfulness of the network signaling, or a trustworthiness of the calling party information, e.g., an ANI or a Caller ID.

Based on the verifying and the determining, the authentication device generates an authentication result indicating whether the calling party number is authenticated and whether that number can be used to authorize the call request. This authentication result can be used by a call processing receiver to, for example, receive and process the call request as an authorized call without further authentication. This procedure both streamlines a caller's experience with the call processing receiver and reduces the processing load on the call processing receiver.

FIG. **1** is a block diagram illustrating a system **100** for call authentication based on calling party information, according to an embodiment. System **100** includes calling party device **102**, service provider network element **104**, communication network **106**, and called party system **110**.

Calling party device **102** is any type of device used to place or receive a telephone call, including, for example, an analog telephone, a digital telephone, a wireless telephone, a computer telephony device, a Voice over Internet Protocol (VOIP) based telephone, or a private branch exchange (PBX) supporting multiple lines or key system supporting multiple lines. Calling party device **102** places a telephone call to called party system **100** via service provider network element **104**.

Service provider network element **104** may include, but is not limited to, analog switches (e.g., 1AESS), digital switches (e.g., 5ESS), IP network switches, or IP network routers. Service provider network element **104** routes telephone calls over communications network **106** to called party system **110**. Communications network **106** includes, for example, wire line or wireless networks, traditional plain old telephone service (POTS) networks, IP-based networks, or any combination or sub-combinations of these types of networks.

In an embodiment, when calling party device **102** places a telephone call to called party system **110**, calling party device **102** transmits a call request containing calling party information, as well as called party information (e.g., a telephone number associated with called party system **110**). Upon receipt of the call request, service provider network element **104** processes the call and provides further signaling to communications network **106** to complete and route the call to called party system **110**. Depending on the type of call and technology of call made by calling party device **102**, service provider network element **104** receives and processes the call request using various network protocols including, but not limited to, Session Initiation Protocol (SIP), Integrated Services Digital Network (ISDN), Plain Old Telephone Service (POTS), Time Division Multiplexing (TDM), or Voice over Internet Protocol (VOIP) call messaging protocols.

In an embodiment, calling party information includes a billing telephone number associated with or assigned to calling party device **102**, information digits that specify a line type (e.g., a class of service), Caller ID (CID) information, or any combination of these. For example, calling party information may be Calling Line Information (CLI), Caller Line Identification (CLID), or Automatic Number Identification (ANI) information. ANI information includes the calling party's billing telephone number and ANI II digits representing the line type of calling party device **102**. Typically, service provider network element **104** is operated by, for example, a telecommunications carrier. Service provider network element **104** sends the calling party information to called party system **110** along with or before the voice portion of the call is transferred to called party system **110**.

Called party system **110** represents systems and devices implemented within a call center or service center of a business entity, such as a bank, that commonly needs to authenticate a calling party's identity. For example, called party system **110** may be a bank-card activation center or a 911 emergency services call center. As shown in FIG. **1**, called party system **110** includes network **112**, call processing receiver **114**, interactive voice response (IVR) device **116**, called party device **118**, authentication device **120**, accounts database **122**, and calling party information database **124**. Each of these components within called party system **110** is implemented by one or more servers.

Call processing receiver **114** is any type of device that processes a call request received from calling party device **102** via communications network **106**. In an embodiment, call processing receiver **114** analyzes received calling party information to determine where to route the call request. For example, call processing receiver **114** may route the received call request to IVR device **116** or called party device **118** via network **112**. Called party device **118** is a device similar to calling party device **102**, but operated by an agent of called party system **110**. Network **112** may represent any wired or wireless network, and may include any combination or sub-combination of local area networks (LANs), wide area networks (WANs), the Internet, POTS, or another wide area data communications network. In an embodiment, call processing receiver **114** is a part of an automatic call distribution (ACD) system or implemented within IVR device **116**.

IVR device **116** interfaces a caller operating calling party device **102** with called party system **110**, e.g., accounts database **122**, without intervention from a human agent. In an embodiment, IVR device **116** interacts with the caller through voice commands instructing the caller to communicate a reason for the telephone call or to select from pre-programmed options via a telephone keypad (e.g., Dual Tone Multifrequency (DTMF) commands). In an embodiment, based on instructions or selections from calling party device **102**, IVR device **116** additionally routes the call request to called party device **118** or retrieve information from accounts database **122**.

When called party system **110** is a business entity, for example, a bank, IVR device **116** requests calling party device **102** to transmit a plurality of personally identifiable (PII) information or other account information before allowing the caller to access information from accounts database **122** or routing the call request to called party device **118**. IVR device **116** receives the transmitted PII as keypad inputs or via voice transmissions. When receiving voice transmissions, IVR device **116** may include voice recognition functions to parse the received PII. As described in the background, PII information may be obtained by unauthorized callers due to security breaches. Thus, not only do traditional IVR device **116** expend significant time and processing power to verify the received PII or account information, but also the verification is unlikely to prevent unauthorized callers, e.g., criminals, from accessing accounts database **122**.

In an embodiment, to reduce the time needed and processing performed by, for example, IVR device **116**, called party system **110** implements authentication device **120**. In an embodiment, some or all of the functionality provided by authentication device **120** is provided by a system external to called party system **110**. For example, a device, operated by a third party, may communicate with called party system **110**, via communication network **106**, to provide the functionality. Authentication device **120** receives a request from call processing receiver **114** to authenticate and pre-authorize an incoming call, i.e., the call request from calling party device **102**, before the call is answered and while the calling party hears one or more ringing tones. In an embodiment, authentication device **120** determines whether the received calling party number can be used as an authentication token, i.e., an ownership token of authentication, for authenticating the call from operating calling party device **102**. But authentication device **120** is not limited to receiving only the calling party number from call processing receiver **114**. In an embodiment, authentication device **120** receives other types of information such as a time of day of the call, trunk number, ANI II digits, dialed number information (DNIS) or called party number, session initiation protocol (SIP) header and routing information, transaction number, unique identifier, or information or data generated by call processing receiver **114** or communications network **106**. In an embodiment, authentication device **120** uses one or more types of the aforementioned information, obtained via communication network **104**, to determine a status, validity, and truthfulness of the network signaling. One or more of these types of information may be received from service provider network element **104** or from a separate device connected to communication network **106**.

In an embodiment, as part of authenticating the calling party number, authentication device **120** queries accounts database **122** for account information associated with the calling party number. Within a bank context, for example, accounts database **122** includes bank account information such as bank transactions, balance information, transfer information, credit limits, and any logged fraud attempts etc. Authentication device **120** compares retrieved account information with a plurality of authentication parameters to determine whether the caller (and associated call request) should be authenticated, further described with respect to FIGS. **3-5**. For example, authentication device **120** may check whether the calling party number associated with the call request is linked to an existing, valid account that has been tagged with a fraud attempt within the past threshold number of days.

In an embodiment, authentication device **120** queries calling party information database **124** for attributes associated with and logged for the calling party number. For example, attributes may include, without limitation, a call frequency, a line type of the calling party number, or a number of accounts linked to the particular account etc. Authentication device **120** similarly compares the queried attributes with the corresponding authentication parameters in determining whether the caller is or should be authenticated, also further described with respect to FIGS. **3-5**.

By authenticating the calling party, authentication device **120** enables devices of called party system **110**, e.g., IVR device **116**, to process the received call as an authenticated call without further processing. In an embodiment, called party system **110**, e.g., IVR device **116**, uses the authentication result to pre-authorize requests associated with the call request without further processing. To do this, in an embodiment, authentication device **120** sends an authentication result including, for example, an authentication token, to call processing receiver **114** that routes the call request based on the result. This authentication token may include, for example, the billing telephone number, such as the ANI number, associated with the calling party. In an embodiment, by treating the billing telephone number as an authentication token, authentication device **120** can authorize future telephones calls associated with this billing telephone number without additional verification.

In an embodiment, if no authentication token was generated, e.g., authentication device **120** did not authenticate the call request based on the calling party information, call processing receiver **114** may route the call request to a device that requires additional input from calling party device **102** to authenticate the caller before authenticating the call.

In an embodiment, authentication device **120** authenticates the calling party of the call request while or after the call has been routed, by call processing receiver **141**, to IVR device **116** or called party device **118**. For example, the authentication process for a particular incoming call may exceed a threshold time. In this case, call processing receiver **114** routes the incoming call to IVR device **116** or called party device **118** before the calling party and associated calling party number has been authenticated by authentication device **120**. In this scenario, authentication device **120** sends to the routed device, such as called party device **118**, a message (e.g., visual or audio) indicating whether the call request and associated calling party is authenticated. For example, authentication device **120** may generate or find an authentication token to associate with the calling party number.

The routed device processes the call request based on the received authentication result. For example, if the result, which may include the authentication token, indicates that the call request cannot be authenticated, IVR device **116** may trigger a script that requires additional information to be provided by the caller. Similarly, called party device **118** receiving a negative result may indicate to an agent via, for example, visual or audio signals that the agent needs to proceed with caution.

FIG. **2** illustrates a distributed system **200** for call authentication based on calling party information, according to an embodiment. Distributed system **200** includes called party device **202**, service provider network element **204**, communications network **206**, called party system **211**, and verification device **230**. In an embodiment, each of the components of distributed system **200** corresponds to the similarly named components of FIG. **1**. For example, called party device **202** places a call to called party system **211** via service provider network element **204**. Then, service provider network element **204** routes the call to called party system **211** via communications network **206**.

In an embodiment, called party system **211** includes multiple called entity **210**A-C, each associated with one or more called telephone numbers. For example, called party system **211** may represent a call center and each of called entity **210**A-C may represent a department, branch, or group within the call center. In an embodiment, each of called entity **210**A-C services a different set of called telephone numbers. Communications network **206** routes a call request to a call processing receiver, such as call processing receiver **214**A, of called entity **210**A based on, for example, the called telephone number within the call request.

Similar to the centralized called party system **110** of FIG. **1**, called entity **210**A may include similarly named components: call processing receiver **214**A, IVR device **216**A, called party device **218**A, accounts database **222**A, and calling party information database **224**A. But in contrast to called party system **110**, authentication device **220** may be centralized across called entity **210**A-C.

Authentication device **220** processes received call requests and associated calling party numbers from any of called entity **210**A-C via respective call processing receivers **214**A-C. In an embodiment, authentication device **220** retrieves information from accounts database **222**A-C and calling party information database **224**A-C across each called entity **210**A-C. In an embodiment, as part of authenticating a received calling party number and authenticating an associated call request, authentication device **220** further distributes processing to verification device **230**.

Verification device **230** may be a component of authentication device **220** or, in an embodiment, part of a system external to called party system **211**. In an embodiment, verification device **230** communicates with authentication device **220** over communications network **206** or another IP-based network, such as the Internet. In an embodiment, to confirm the credibility and validity of a calling party number, verification device **230** is coupled to one or more service provider network element **204** via, for example, communications network **206**. By doing so, verification device **230** may receive various types of information to determine a truthfulness of the network signalling from communications network **206**. For example, the information may include a time of day of the call, trunk number, ANI II digits, dialed number information (DNIS) or called party number, session initiation protocol (SIP) header and routing information, transaction number, unique identifier, or information or data generated by call processing receiver **214**A-C.

In an embodiment, upon receiving a calling party number, verification device **230** determines the calling party number is valid based on calling party number attributes or an operating status of the calling party number. In an embodiment, to authenticate the caller and associated call request, verification device **230** must determine that the associated calling party number is valid. In an embodiment, verification device **230** verifies, in part, the calling party number after determining that the calling party number originates from a known physical location assigned to or associated with the calling party number. In an embodiment, verification device **230** verifies, in part, the calling party number after determining that the calling party number originates from a type of the calling device, e.g., a physical device such as a handset, known to be associated with or assigned to the calling party number. To do this, verification device **230** may place an outbound call to the calling party number and analyze an operating status of the outbound call. In an embodiment, verification device **230** determines that a calling party number should not be verified based on a type of the device, e.g., a prison phone, a payphone, a phone associated with a large company, etc.

In an embodiment, in addition to determining a validity or credibility of a calling party number, verification device **230** determines a credibility score, i.e., a trustworthiness level, indicating how likely that the calling party number is valid based on various calling party number parameters, the operating status, among other related information received from, for example, service provider network element **204**. For example, verification device **230** may be implemented similar to the methods and systems described in U.S. Pat. No. 8,238,532B1, titled "Method and System for Discovering and Reporting Trustworthiness and Credibility of Calling Party Number Information," which is incorporated by reference herein in its entirety.

FIG. **3** is a block diagram illustrating a system **300** for authenticating calling party information for authenticating a call, according to an embodiment. System **300** includes authentication device **302** coupled to accounts database **320** and calling party information database **330**. Authentication device **302** is an example implementation of authentication device **120** from FIG. **1** or an example of a centralized device serving a plurality of distributed called entities, as further described with respect to authentication device **220** of FIG. **2**.

Accounts database **320** includes account **322** managed or provided by a called party system, such as called party system **110** of FIG. **1**. Accounts database **320** also stores information related to account **322** including, without limitation, a unique account identifier (ID), PII of account holder (e.g., an account holder's legal name or date of birth), one or more calling party numbers linked with one or more account **322**, account age, account standing, whether a credit limit has been exceeded, or transaction history. Accounts database **320** may also include fraud history **324** associated with account **322**. In an embodiment, fraud history **324** includes one or more of: logged occurrences of fraud for account **322**, associated dates of fraud, a type of fraud logged for or associated with account **322**, a location of the fraud, a severity of the fraud, or a date or time when fraud was identified or logged, or a combination thereof. In some embodiments, fraud history **324** further includes statistical analysis of logged instances of fraud related to a number of the fraud occurrences or fraud types, The type of fraud may be a means by which fraud was performed or detected including, for example, by telephone call, by web portal, by ATM, or by physical transaction with an agent (e.g., with a bank teller). In an embodiment, one or more designated types of fraud, e.g., ATM fraud, associated with a linked account **322** do not negatively affect an authentication result generated by authentication device **302**. Further, a fraud type may include a severity of the fraud where fraud with designated dollar amounts is classified as a type of fraud, e.g., low-severity fraud type versus high-severity fraud type. In an embodiment, accounts database **320** includes, in part, account information and fraud history retrieved across a plurality of databases, such as accounts database **222**A-C within called party system **211** of FIG. **2**.

Calling party information database **330** includes calling party number **332**, such as a calling party number or billing number from ANI received in calling party information. In an embodiment, for each calling party number **332**, calling party information database **330** stores associated authentication history **334**, attributes **336**, or linked accounts **338**. In an embodiment, calling party information database **330** includes or represents, in part, calling party information from calling party device **218**A-C across called entity **210**A-C of FIG. **2**. In an embodiment, calling party information database **330** includes information received from, for example, service provider network element **204** of FIG. **2**.

In an embodiment, authentication history **334** includes whether the calling party number had been successfully authenticated in the past, and how long ago the authentication or authentication was performed. For example, a calling party number may be authenticated as a valid calling number from a known physical calling device, but the calling party number may not have been previously linked to or associated with any existing valid accounts. Therefore, for example, the calling number may be valid but not authenticated. In an embodiment, authentication history **334** stores information indicating that a calling party number was previously authenticated in which case the received calling party is used as an authentication token for authenticating, and possibly authorizing, the call request without requesting additional information from the calling party.

In an embodiment, attributes **336** includes calling attributes associated with calling party number **332**. For example, attributes **336** may include, without limitation, a frequency of calls (e.g., a number of calls within a threshold timeframe that originates from calling party number **332**), a velocity of calls (e.g., how frequently calls are allegedly originating from calling party number **332**), or a line type (e.g., a landline, an IP phone, a cellular phone, etc.). In an embodiment, linked accounts **338** includes the number of accounts currently linked to calling party number **332** or the specific accounts themselves. Linked accounts **338** may also include information indicating a status of the accounts, e.g., an account has not been closed.

In an embodiment, calling party information database **330** includes a table of line type **340** that authentication device **302** may query to, for example, determine a line type of a specific calling party number **332**. For example, authentication device **302** may query line type **340** based on the ANI II digits of an ANI within the call request. In an embodiment, line type **340** includes, without limitation, a landline POTS line, a multiparty line, unassigned, a toll-free line, a payphone line, a prison/inmate service line, a cellular/wireless line, an IP phone line, or other line types. In an embodiment, authentication device **302** determines whether a calling party number should be authorized based on the identified line type.

Authentication parameters **314** include one or more thresholds used by the components of authentication device **302** to determine whether a calling party number (and associated call request) can be authenticated. In an embodiment, the authentication result is used to determine whether the associated call request should be authorized. In an embodiment, authentication parameters **314** stores one or more thresholds for one or more parameters stored in accounts database **320** and calling party information database **330**. For example, for a frequency of calls (an example parameter) stored in attributes **336**, a stored threshold may be 10 calls within the past 24 hours. Authentication device **302**, e.g., calling number authenticator **306**, may determine that, for example, a call request should not be authenticated if the number of calls associated with the calling number exceeds the threshold of 10 calls within the past 24 hours. In an embodiment, authentication parameters **314** stores multiple thresholds for the same parameter conditioned on a classification of the calling party number. For example, authentication parameters **314** may store different thresholds for each line type such that some line types (known to be associated with lower fraud) have more lenient thresholds.

In an embodiment, to authenticate a received calling number, authentication device **302** implements the following components: calling number verificator **304**, calling number authenticator **306**, authentication parameter tuner **308**, and communications interface **310**. Each component may include a selection of stored operations that when executing in the one or more processors of authentication device **302** causes the one or more processors to perform the operations of that component.

Communications interface **310** is configured to enable network communications between authentication device **302** and one or more the devices and components of FIG. **1**, such as call processing receiver **114**, IVR device **116**, or called party device **118**, or FIG. **2**, such as called entity **210**A-C. For example, communications interface **310** may connect to network **112** of FIG. **1** or networks **212**A-C of FIG. **2**. In an embodiment, communications interface **310** connects to, for example, communications network **206** to retrieve information from, for example, service provider network element **204** of FIG. **2**. In an embodiment, communications interface **310** transmits an authentication result to, for example, call processing receiver **114** of FIG. **1** before the call request is routed by call processing receiver **114**. If the call has been routed, communications interface **310** transmits the authentication result to the routed device, such as IVR device **116** or called party device **118** of FIG. **1**. In an embodiment, the routed device, such as call processing receiver **114** or IVR device **116**, uses the authentication result to authorize the call request.

Calling number verificator **304** verifies the call request by verifying that the call request originates from the purported calling party number. In an embodiment, calling number verificator **304** receives the calling party number and associated information from, for example, call processing receiver **114** of FIG. **1**. The calling party number and associated information may include ANI or Caller ID information.

To determine whether the calling party number is valid, calling number verificator **304** may perform ANI analysis while the caller's calling device, such as calling party device **102** of FIG. **1**, is in an actual or virtual on-hook condition and an answered condition. In an embodiment, to perform ANI analysis, calling number verificator **304** queries calling party information database **330** for attributes **336** associated with calling party number **332** corresponding to the received calling party number. Additionally or alternatively, calling number verificator **304** may receive one or more attributes from service provider network element **104** of FIG. **1**.

Then, calling number verificator **304** may compare one or more attributes **336** with corresponding thresholds or requirements of authentication parameters **314**. For example, calling number verificator **304** may check that the calling party number's line type (an example attribute **336**) is of a line type within authentication parameters **314** and that the frequency of calls (an example attribute **336**) is below the threshold specified in authentication parameters **314**. Calling number verificator **304** additionally checks a format of the calling number, e.g., that it includes 10 digits.

In an embodiment, when the calling party number is a line associated with or assigned a static physical location, calling number verificator **304** verifies calling party number as valid by verifying that the calling party number originates from that physical location. For example, calling number verificator **304** may compare an originating switch identifier with the NPA-NXX (area code/exchange) digits of the calling party number.

In an embodiment, calling number verificator **304** verifies the calling party number based on, in part, verifying that the calling party number originates from a physical calling device or a device type assigned to or associated with the calling party number. To do this, calling number verificator **304** may query a network condition or a call operational status while placing one or more outbound calls to the calling party number, e.g., the telephone number represented by an ANI of the call request. In an embodiment, calling number verificator **304** places the one or more outbound calls before the call request is processed or answered. Example network conditions may include busy, ring then answer, call forward then answer, or ringing no answer. Further descriptions of the ANI analysis including, for example, gathering other types of network conditions are provided in the '532 patent.

In an embodiment, calling number verificator **304** requests a separate device such as verification device **230** of FIG. **2** to perform the authentication. In this embodiment, calling number verificator **304** is an interface to, for example, verification device **230**.

Calling number authenticator **306** determines whether an incoming call request received from, for example, call processing receiver **214**A of FIG. **2**, should be authenticated based, in part, on the verification result generated by calling number verificator **304** that verifies a received calling party number is valid. In an embodiment, calling number authenticator **306** queries calling party information database **330** for linked accounts **338** of calling party number **332** corresponding to the calling party number of the call request. Calling number authenticator **306** may also retrieve one or more of authentication history **334** or attributes **336** associated with calling party number **332**. For each of linked accounts **338** that has been identified, calling number authenticator **306** also queries accounts database **320** for fraud history **324** and other information associated with each identified account **322**. In an embodiment, to determine whether to authenticate the calling party associated with the call request, calling number authenticator **306** checks whether one or more portions of received information satisfy the thresholds or requirements of authentication parameters **314**. In an embodiment, calling number authenticator **306** generates a message indicating that the calling party of the call request is authenticated or not authenticated.

Additionally or alternatively, calling number authenticator **306** may compute a risk score (or confidence score) based on whether specific portions of received information satisfy the thresholds or requirements of authentication parameters **314**. For example, a risk score may range from 1 (highest risk) to 5 (lowest risk), though other ranking schemes would be apparent to one skilled in the art. In an embodiment, calling number authenticator **306** selects a maximum risk score, i.e., a risk threshold, for authenticating the call request based, in part, on a line type of the calling party number or a reason for the call. For example, a landline or mobile line type may be associated with a lower maximum risk score than compared to an IP phone or payphone. In an embodiment, calling number authenticator **306** determines the reason for the call based on, for example, the dialed number (DNIS) or additional information (e.g., keypad inputs or voice inputs) received from calling party device **102**. For example, a request to check a balance of account **322** may be associated with a lower maximum risk score than compared to adding a member to account **322**. In an embodiment, the calculated risk score is affected by the verification result generated by calling number verificator **304**.

To generate an authentication result using the computed risk score, calling number authenticator **306** compares the computed risk score with the maximum risk score selected for the current received call request. When the computed risk score is less than or equal to the maximum risk score, calling number authenticator **306** authenticates the calling party number and associated call request. In an embodiment where the call request is authenticated before it is answered, calling number authenticator **306** sends an authentication result to a call processing receiver that originated the request, such as call processing receiver **214**A of FIG. **2**, to authorize the call request. In an embodiment, calling number authenticator **306** sends an authentication result after the call request has been routed by the call processing receiver and answered by an IVR device or a called party device. In this case, calling number authenticator **306** sends the message to the routed device that processes the call request based on the authentication result. For example, an IVR device that receives a negative authentication result, which indicates the call request should not be authorized, may run one or more scripts requesting the caller to submit PII to verify his or her identity. Further embodiments are described with respect to FIGS. **4**-**6**.

Authentication parameter tuner **308** adjusts one or more thresholds or requirements of authentication parameters **314** to increase how accurate calling number authenticator **306** is in determining whether a given calling party number can authenticate a call request. Particularly, authentication parameter tuner **308** determines that calling number authenticator **306** fails to correctly authenticate a call request when fraud is subsequently logged or determined for an authenticated call request. In an embodiment, authentication parameter tuner **308** additionally fails to correctly authenticate a call request when calling number authenticator **306** fails to authenticate a call request that is subsequently determined to be fraud-free. In an embodiment, to reduce fraud, authentication parameter tuner **308** adjusts one or more thresholds or requirements of authentication parameters **314** to reduce incorrectly authenticated call requests, i.e., authenticated call requests that are subsequently associated with fraud.

FIG. **4** is a flow chart of a method **400** for generating an authentication result, according to an embodiment. In an embodiment, method **400** is performed by authentication device **302** of FIG. **3**. For ease of reference, method **400** will be described with respect to the components of authentication device **302**.

Method **400** starts at step **402**. In step **402**, calling number verificator **304** receives a call request from a call processing receiver, such as call processing receiver **114** of FIG. **1**. The call request includes at least a called party number and calling party information, which may include a calling party number. In an embodiment, the calling party information includes, but is not limited to, ANI information or caller ID information.

In step **404**, calling number authenticator **306** queries calling party information database **330** to retrieve linked accounts **338**, attributes **336**, or authentication history **334** information for calling party number **332** corresponding to the received calling party number, e.g., within ANI. Additionally, calling number authenticator **306** queries accounts database **320** to retrieve fraud history **324** information for each account **332** identified in linked accounts **338**.

In step **406**, calling number verificator **304** determines a result of calling party number verification. In an embodiment, calling number verificator **304** determines whether the calling party number can be verified as a valid number. For example as described with respect to FIG. **3**, calling number verificator **304** may verify that the calling party number has not been spoofed by placing an outbound call to the calling party number and analyzing the operating status of the call. In an embodiment, calling number verificator **304** verifies a validity of the call request based on whether the call request originates from a location or a device associated with the calling party number. In an embodiment, the verification result is a credibility score indicating how likely the calling party number is valid. In an embodiment as depicted with respect to FIG. **2** and described with respect to FIG. **3**, calling number verificator **304** requests an external verification device to perforin the verifying.

In steps **408**-**412**, calling number authenticator **306** compares a plurality of information related to the calling party number with corresponding thresholds or requirements within authentication parameters **314** to determine whether the calling party number can be used to authorize the call request. For example, the plurality of information may be information retrieved by calling number authenticator **306** in step **404**.

In step **408**, calling number authenticator **306** checks whether one or more queried attributes **336** satisfy the thresholds or rules stored within authentication parameters **314**. For example, calling number authenticator **306** may determine whether a line type of the calling number is one of the acceptable line types specified in authentication parameters **314**. Further, calling number authenticator **306** may compare a queried call velocity with a maximum threshold (which may depend on an identified line type) retrieved from authentication parameters **314**. In an embodiment, calling number authenticator **306** tracks a number of queried attributes **336** that satisfy the corresponding thresholds or rules within authentication parameters **314**.

In step **410**, calling number authenticator **306** determines whether the retrieved number of linked accounts **338** is between one and a threshold value, inclusive, in authentication parameters **314**. In an embodiment, if the number of linked accounts **338** exceeds the corresponding threshold value from authentication parameters **314**, calling number authenticator **306** determines that the call request cannot be authenticated. In an embodiment, the threshold value noted above may vary depending on values of other identified parameters, such as whether the calling party number is of a specific line type, a purpose of the call request, or whether the calling party number has been authenticated or authorized within a time period, etc.

In step **412**, calling number authenticator **306** checks fraud history **324** of each account **322** linked to the calling party number. Like steps **408**-**410**, calling number authenticator **306** may compare logged fraud history **324** with authentication parameters **314**. For example, calling number authenticator **306** may authenticate the call request based on whether any fraud attempt has been logged with any linked account **322** within the last month, or another specified number of days.

In step **414**, calling number authenticator **306** generates an authentication result based on the results of steps **406-412**. Therefore, calling number authenticator **306** may factor the verification result of step **406** in determining the authentication result. The authentication result includes information indicating whether the call request and associated calling party or caller is authenticated. In an embodiment, calling number authenticator **306** authenticates the call request if calling number verificator **304** verified the validity of the call request and a certain number of checked parameters (in steps **408-412**) meets the corresponding thresholds and rules of authentication parameters **314**. For example, the call request is verified when the calling party number, e.g., ANI number, is valid as explained in step **406**. In an embodiment, if any check or verification performed by steps **406-412** fails, calling number authenticator **306** generates an authentication result indicating that the call request is not authenticated. For example, if the number of accounts linked to the calling party number exceeds a threshold value, then calling number authenticator **306** generates an authentication result indicating that the call request is not authenticated. In an embodiment, one of the checked parameters that needs to be met is whether the number of accounts linked to the calling party number is between one and a threshold value, inclusive.

In an embodiment, calling number authenticator **306** calculates a confidence score based on the results of steps **406-112**. Each of the results may be weighted differently. For example, a verification result may have a larger impact on the confidence score than, for example, a check on the frequency of calls associated with the calling party number. In an embodiment, a result to be used in calculating the confidence score includes whether the calling party number had been previously authenticated within the past month, or other threshold number of days.

To generate an authentication result, calling number authenticator **306** may compare the calculated confidence score with a risk threshold retrieved from authentication parameters **314**. The risk threshold may be retrieved based on one or more queried values of parameters. For example, calling number authenticator **306** may retrieve a different risk threshold based on a line type identified for the calling party number. Calling number authenticator **306** may authenticate the call, for example, when the confidence score exceeds the retrieved risk threshold.

In step **416**, calling number authenticator **306** updates accounts database **320** and calling party information database **330** to enable authentication parameter tuner **308** to (periodically or on-demand) adjust one or more authentication parameters **314**. For example, calling number authenticator **306** may save the authentication result in authentication history **334** of calling party information database **330**.

In step **418**, calling number authenticator **306** sends the authentication result to the call processing receiver, such as call processing receiver **114** of FIG. **1**. The call processing receiver uses the authentication result to accurately and efficiently process the call request. For example, when the authentication result indicates that the call request is authenticated, the call processing receiver may immediate authorize the received and routed call request without requesting, e.g., via an automated voice message, additional information from the caller. Therefore, the call processing receiver provides a streamlined interface without unnecessary voice or button-press processing, depending on how the additional information is input from the caller. In contrast, when the authentication result indicates that the call request is not authenticated, not only is the call request not authorized, the call processing receiver may request additional information to authenticate the caller of the call. In an embodiment, when the call request was routed by the call processing receiver to an IVR device or a called party device, calling number authenticator **306** forwards the authentication result to the routed device.

FIG. **5** is a flow chart of a method **500** for improving accuracy of generating authentication results, according to an embodiment. In an embodiment, steps of method **500** may be performed by authentication device **302** of FIG. **3**. For ease of reference, steps of method **500** will be described with respect to the components of authentication device **302**. In an embodiment, authentication parameter tuner **308** performs the steps of method **500** periodically, when an accuracy of calling number authenticator **306** falls below a threshold, or when a fraud rate increases above a threshold.

Method **500** starts in step **502**. In step **502**, authentication parameter tuner **308** tracks account and fraud information aggregated across a plurality of databases, for example, databases of called entities **210**A-C in FIG. **2**.

In step **504**, authentication parameter tuner **308** saves or logs authentication results generated by calling number authenticator **306** for each call request and associated calling party number. In an embodiment, calling number authenticator **306** also saves or logs the authentication results in authentication history **334** for calling party number **332**.

In step **506**, authentication parameter tuner **308** analyzes the authentication results of step **504** with respect to fraud identified for one or more previously authenticated call requests. In an embodiment, the analysis includes computing and tracking an accuracy rate of calling number authenticator **306** using a set of configured authentication parameters **314**.

In step **508**, responsive to the analysis of step **506**, authentication parameter tuner **308** adjusts one or more authentication parameters **314** to increase the accuracy rate of calling number authenticator **306** or to decrease the rate of fraud. In an embodiment, authentication parameter tuner **308** makes adjustments based on a history of logged accuracy rates and fraud rates for each set of configured authentication parameters **314** as well as previous adjustments made to authentication parameters **314**. For example, calling number authenticator **306** may decrease a threshold for the number of linked accounts (an example of authentication parameters **314**) when the previous adjustment to decrease the threshold decreased the overall fraud rate or increased the accuracy rate of calling number authenticator **306**.

Various embodiments, such as embodiments described with respect to devices or systems of FIGS. **1-3**, can be implemented, for example, using one or more well-known computer systems, such as computer system **700** shown in FIG. **7**. Computer system **700** can be any well-known computer capable of performing the functions described herein.

Computer system **700** includes one or more processors (also called central processing units, or CPUs), such as a processor **704**. Processor **704** is connected to a communication infrastructure or bus **706**.

One or more processors **704** may each be a graphics processing unit (GPU). In an embodiment, a GPU is a processor that is a specialized electronic circuit designed to process mathematically intensive applications. The GPU may have a parallel structure that is efficient for parallel processing of large blocks of data, such as mathematically intensive data common to computer graphics applications, images, videos, etc.

Computer system **700** also includes user input/output device(s) **703**, such as monitors, keyboards, pointing devices, etc., that communicate with communication infrastructure **706** through user input/output interface(s) **702**.

Computer system **700** also includes a main or primary memory **708**, such as random access memory (RAM). Main memory **708** may include one or more levels of cache. Main memory **708** has stored therein control logic (i.e., computer software) or data.

Computer system **700** may also include one or more secondary storage devices or memory **710**. Secondary memory **710** may include, for example, a hard disk drive **712** or a removable storage device or drive **714**. Removable storage drive **714** may be a floppy disk drive, a magnetic tape drive, a compact disk drive, an optical storage device, tape backup device, or any other storage device/drive.

Removable storage drive **714** may interact with a removable storage unit **718**. Removable storage unit **718** includes a computer usable or readable storage device having stored thereon computer software (control logic) or data. Removable storage unit **718** may be a floppy disk, magnetic tape, compact disk, DVD, optical storage disk, and/any other computer data storage device. Removable storage drive **714** reads from or writes to removable storage unit **718** in a well-known manner.

According to an exemplary embodiment, secondary memory **710** may include other means, instrumentalities or other approaches for allowing computer programs or other instructions or data to be accessed by computer system **700**. Such means, instrumentalities or other approaches may include, for example, a removable storage unit **722** and an interface **720**. Examples of the removable storage unit **722** and the interface **720** may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an EPROM or PROM) and associated socket, a memory stick and USB port, a memory card and associated memory card slot, or any other removable storage unit and associated interface.

Computer system **700** may further include a communication or network interface **724**. Communication interface **724** enables computer system **700** to communicate and interact with any combination of remote devices, remote networks, remote entities, etc. (individually and collectively referenced by reference number **728**). For example, communication interface **724** may allow computer system **700** to communicate with remote devices **728** over communications path **726**, which may be wired or wireless, and which may include any combination of LANs, WANs, the Internet, etc. Control logic or data may be transmitted to and from computer system **700** via communication path **726**.

In an embodiment, a tangible apparatus or article of manufacture comprising a tangible computer useable or readable medium having control logic (software) stored thereon is also referred to herein as a computer program product or program storage device. This includes, but is not limited to, computer system **700**, main memory **708**, secondary memory **710**, and removable storage units **718** and **722**, as well as tangible articles of manufacture embodying any combination of the foregoing. Such control logic, when executed by one or more data processing devices (such as computer system **700**), causes such data processing devices to operate as described herein.

Based on the teachings contained in this disclosure, it will be apparent to persons skilled in the relevant art(s) how to make and use embodiments of the invention using data processing devices, computer systems or computer architectures other than that shown in FIG. **7**. In particular, embodiments may operate with software, hardware, or operating system implementations other than those described herein.

It is to be appreciated that the Detailed Description section, and not the Summary and Abstract sections (if any), is intended to be used to interpret the claims. The Summary and Abstract sections (if any) may set forth one or more but not all exemplary embodiments of the invention as contemplated by the inventor(s), and thus, are not intended to limit the invention or the appended claims in any way.

While the invention has been described herein with reference to exemplary embodiments for exemplary fields and applications, it should be understood that the invention is not limited thereto. Other embodiments and modifications thereto are possible, and are within the scope and spirit of the invention. For example, and without limiting the generality of this paragraph, embodiments are not limited to the software, hardware, firmware, or entities illustrated in the figures or described herein. Further, embodiments (whether or not explicitly described herein) have significant utility to fields and applications beyond the examples described herein.

Embodiments have been described herein with the aid of functional building blocks illustrating the implementation of specified functions and relationships thereof. The boundaries of these functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternate boundaries can be defined as long as the specified functions and relationships (or equivalents thereof) are appropriately performed. Also, alternative embodiments may perform functional blocks, steps, operations, methods, etc. using orderings different than those described herein.

References herein to "one embodiment," "an embodiment," "an example embodiment," or similar phrases, indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it would be within the knowledge of persons skilled in the relevant art(s) to incorporate such feature, structure, or characteristic into other embodiments whether or not explicitly mentioned or described herein.

The breadth and scope of the invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

What is claimed is:

1. A method, comprising:

receiving, by an authentication device, a call request and associated calling party information that includes a calling party number, wherein the call request is initiated by a caller;

retrieving, by the authentication device, parameters associated with the calling party number, wherein the parameters include a number of accounts linked to the calling party number;

determining whether the number of accounts is between one and a threshold value, inclusive;

authenticating, by the authentication device, the calling party number by verifying that the call request originates from a location or a device associated with the calling party number;

generating, by the authentication device based on the verifying and whether the number of accounts is determined to be between one and the threshold value, an authentication result indicating whether the calling party number is authenticated; and

sending, by the authentication device, the authentication result to a call processing device that processes the call request from the caller according to the authentication result.

2. The method of claim **1**, wherein an authenticated calling party number authenticates the caller before the call processing device connects to the caller.

3. The method of claim **1**, the verifying comprising:

requesting a verification system to perform the verifying, wherein the verification system analyzes an operational status of the call.

4. The method of claim **1**, the generating comprising:

generating an authentication result that indicates the calling party number cannot be authenticated responsive to determining that the number of accounts exceeds the threshold value or that the call request originates from a location or a device not associated with the calling party number.

5. The method of claim **1**, the generating comprising:

using a result of the verifying and the determining to compute a risk score indicating how likely the call request is associated with fraud; and

comparing the risk score with a risk threshold to determine the authentication result.

6. The method of claim **5**, the comparing comprising:

retrieving the risk threshold based on one or more of the retrieved parameters, wherein a retrieved parameter includes a line type of the calling party number.

7. The method of claim **5**, the generating further comprising:

retrieving fraud information associated with each of the linked accounts; and

computing the risk score based on whether any fraud associated with one of the accounts is within a threshold number of days.

8. The method of claim **7**, wherein the parameters include retrieved fraud information, the generating further comprising:

computing the risk score based on how many of the retrieved parameters meets corresponding thresholds used in authenticating the calling party number of the caller.

9. The method of claim **8**, wherein the parameters retrieved for information associated with the calling party number includes one or more of a time of day, a frequency of calls, a velocity of calls, or a line type.

10. The method of claim **7**, further comprising:

tracking the number of accounts linked to the calling party number and fraud information associated with each of the linked accounts;

associating the authentication result with the calling party number; and

adjusting one or more thresholds corresponding to the retrieved parameters based on an accuracy of the authentication result.

11. The method of claim **1**, further comprising:

sending the authentication result to the call processing device as a visual or audio indication.

12. A system, comprising:

a memory for storing a plurality of thresholds corresponding to a plurality of parameters;

a processor coupled to the memory;

a communications interface that when executing in the processor receives a call request and associated calling party information that includes a calling party number, wherein the call request is initiated by a caller;

a calling number verificator that when executing in the processor:

verifies that the call request originates from a location or a device associated with the calling party number;

a calling number authenticator that when executing in the processor:

retrieves the plurality of parameters associated with the calling party number, wherein the parameters include a number of accounts linked to the calling party number,

determines whether the number of accounts is between one and a threshold value, inclusive;

generates, based on the verifying and whether the number of accounts is determined to be between one and the threshold value, inclusive, an authentication result indicating whether the calling party number is authenticated, and

sends the authentication result to a call processing device that processes the call request from the caller according to the authentication result.

13. The system of claim **12**, wherein an authenticated calling party number authenticates the caller before the call processing device connects to the caller.

14. The system of claim **12**, wherein the calling number verificator further:

requests a verification system to perform the verifying, wherein the verification system analyzes an operational status of the outbound call.

15. The system of claim **12**, wherein the calling number authenticator further:

uses a result of the verifying and the determining to compute a risk score indicating how likely the call request is associated with fraud; and

compares the risk score with a risk threshold to determine the authentication result.

16. The system of claim **15**, wherein the calling number authenticator further:

retrieves the risk threshold based on one or more of the retrieved parameters, wherein a retrieved parameter includes a line type of the calling party number.

17. The system of claim **15**, wherein the calling number authenticator further:

retrieves fraud information associated with each of the linked accounts; and

computes the risk score based on whether any fraud associated with one of the accounts is within a threshold number of days.

18. The system of claim **17**, wherein the parameters includes retrieved fraud information, and wherein the calling number authenticator further:

computes the risk score based on how many of the retrieved parameters meets corresponding thresholds used in authenticating the calling party number of the caller.

19. The system of claim **18**, wherein the parameters retrieved for information associated with the calling party number includes one or more of a time of day, a frequency of calls, a velocity of calls, or a line type.

20. A non-transitory computer-readable device having instructions stored thereon that, when executed by at least one computing device, causes the at least one computing device to perform operations comprising:

receiving, by an authentication device, a call request and associated calling party information that includes a calling party number, wherein the call request is initiated by a caller;

retrieving, by the authentication device, parameters associated with the calling party number, wherein the parameters include a number of accounts linked to the calling party number;

determining whether the number of accounts is between one and a threshold value, inclusive;

verifying, by the authentication device, that the call request originates from a location or a device associated with the calling party number;

generating, by the authentication device based on the verifying and whether the number of accounts is determined to be between one and the threshold value, inclusive, an authentication result indicating whether the calling party number is authenticated; and

sending, by the authentication device, the authentication result to a call processing device that processes the call request according to the authentication result, wherein an authenticated calling party number authenticates the caller.

* * * * *

Exhibit 5

US010693840B2

(12) **United States Patent**
Peterson et al.

(10) **Patent No.: US 10,693,840 B2**
(45) **Date of Patent: *Jun. 23, 2020**

(54) **METHOD FOR DISTRIBUTING CONTACT INFORMATION BETWEEN APPLICATIONS**

(71) Applicant: **Neustar, Inc.**, Sterling, VA (US)

(72) Inventors: **Jon Peterson**, Sterling, VA (US); **Webb Dryfoos**, Sterling, VA (US); **Peter Charlier Davis**, Sterling, VA (US)

(73) Assignee: **Neustar, Inc.**, Sterling, VA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/178,915**

(22) Filed: **Nov. 2, 2018**

(65) **Prior Publication Data**

US 2019/0239783 A1 Aug. 8, 2019

Related U.S. Application Data

(63) Continuation of application No. 15/487,178, filed on Apr. 13, 2017, now Pat. No. 10,117,609, which is a continuation of application No. 12/705,268, filed on Feb. 12, 2010, now Pat. No. 9,636,053.

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/04*** (2013.01); ***H04L 67/104*** (2013.01); *H04L 29/08306* (2013.01)

(58) **Field of Classification Search**
CPC ... H04L 61/1594; H04L 63/04; H04L 67/104; H04L 67/306; H04L 29/08306
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

9,636,053	B2 *	5/2017	Peterson	A61B 5/14546
10,117,609	B2 *	11/2018	Peterson	A61B 5/14546
2002/0049828	A1	4/2002	Pekarek-Kostka	
2002/0152265	A1 *	10/2002	Felman	G06Q 10/10 709/203
2003/0177246	A1 *	9/2003	Goodman	H04L 67/104 709/228
2003/0186704	A1	10/2003	Tamura et al.	
2005/0066219	A1 *	3/2005	Hoffman	G06F 21/6218 714/4.1
2005/0266835	A1	12/2005	Agrawal et al.	
2007/0038720	A1	2/2007	Reding et al.	
2008/0232371	A1 *	9/2008	Hildreth	H04L 12/1813 370/392

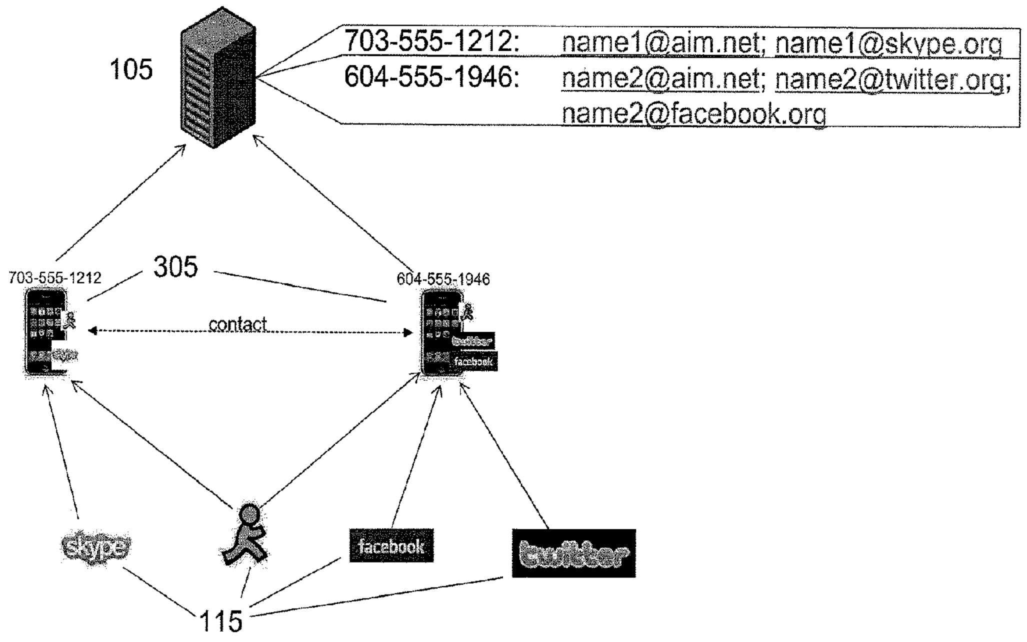
(Continued)

Primary Examiner — Walli Z Butt
Assistant Examiner — Ryan C Kavleski
(74) *Attorney, Agent, or Firm* — Sterne, Kessler, Goldstein & Fox P.L.L.C.

(57) **ABSTRACT**

A method and system for distributing contacting information between applications is provided. The system preferably uses an ENUM-type protocol and a middleware tool kit to associate telephone numbers to other identifying information, such as e-mail addresses or URLs for web sites. The system enables the associated contacting information to be shared across multiple applications that may be implemented on a computer or a mobile telephony device. Information is shared only after verification that a requester is authorized to receive the requested contacting information.

20 Claims, 4 Drawing Sheets


105
703-555-1212: name1@aim.net; name1@skype.org
604-555-1946: name2@aim.net; name2@twitter.org; name2@facebook.org
703-555-1212
305
604-555-1946
contact
twitter
facebook
skype
facebook
twitter
115

(56) **References Cited**

U.S. PATENT DOCUMENTS

2009/0089292	A1	4/2009	Cheah
2010/0082761	A1	4/2010	Nguyenphu et al.
2011/0201312	A1	8/2011	Peterson et al.
2012/0009902	A2	1/2012	Peterson et al.
2012/0016939	A1	1/2012	Cheah
2017/0281061	A1	10/2017	Peterson et al.

* cited by examiner

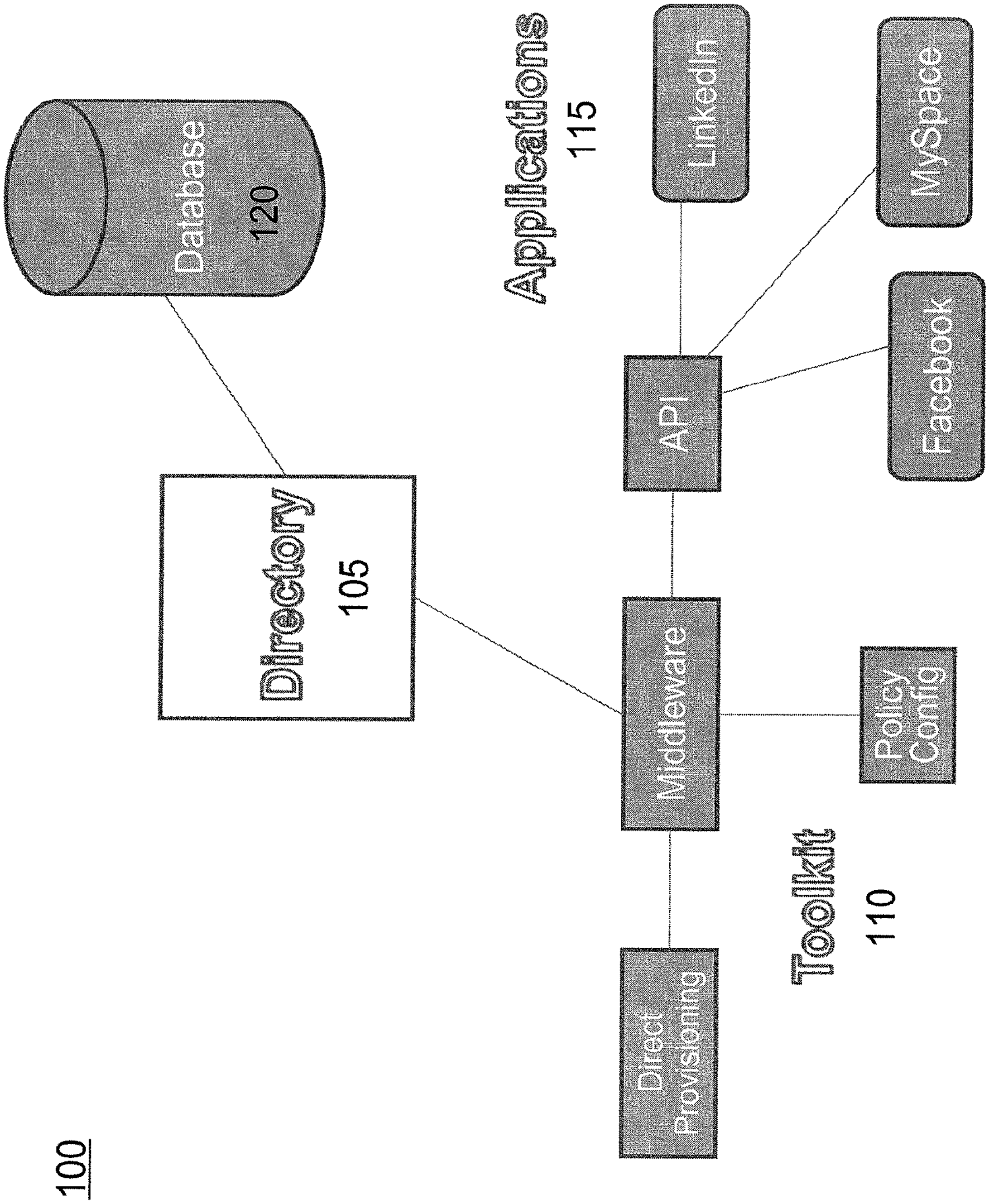

100
Database
120
Directory
105
Applications
115
LinkedIn
MySpace
Facebook
API
Middleware
Policy Config
Direct Provisioning
Toolkit
110

Fig. 1

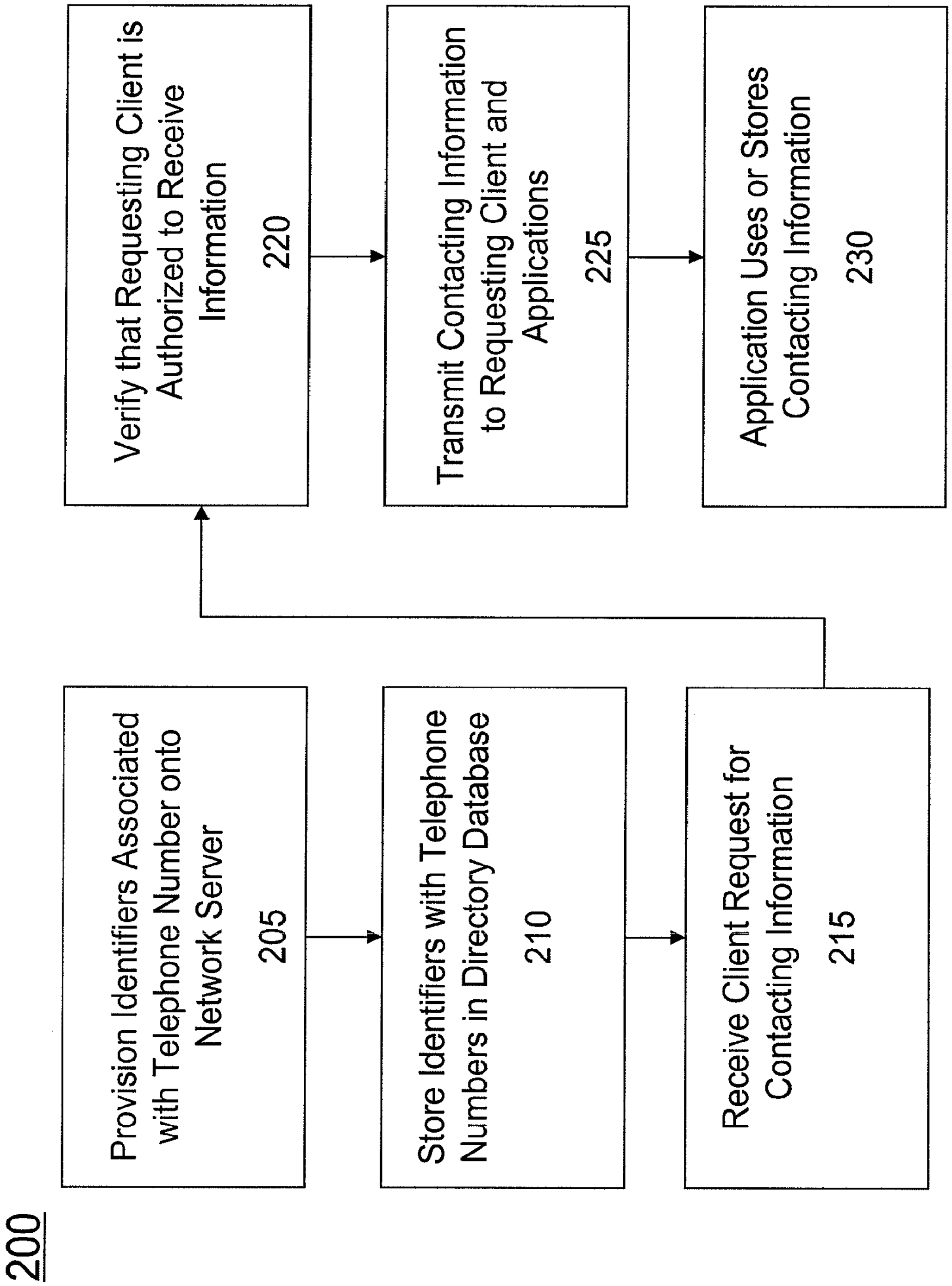

200
Provision Identifiers Associated with Telephone Number onto Network Server
205
Store Identifiers with Telephone Numbers in Directory Database
210
Receive Client Request for Contacting Information
215
Verify that Requesting Client is Authorized to Receive Information
220
Transmit Contacting Information to Requesting Client and Applications
225
Application Uses or Stores Contacting Information
230

Fig. 2

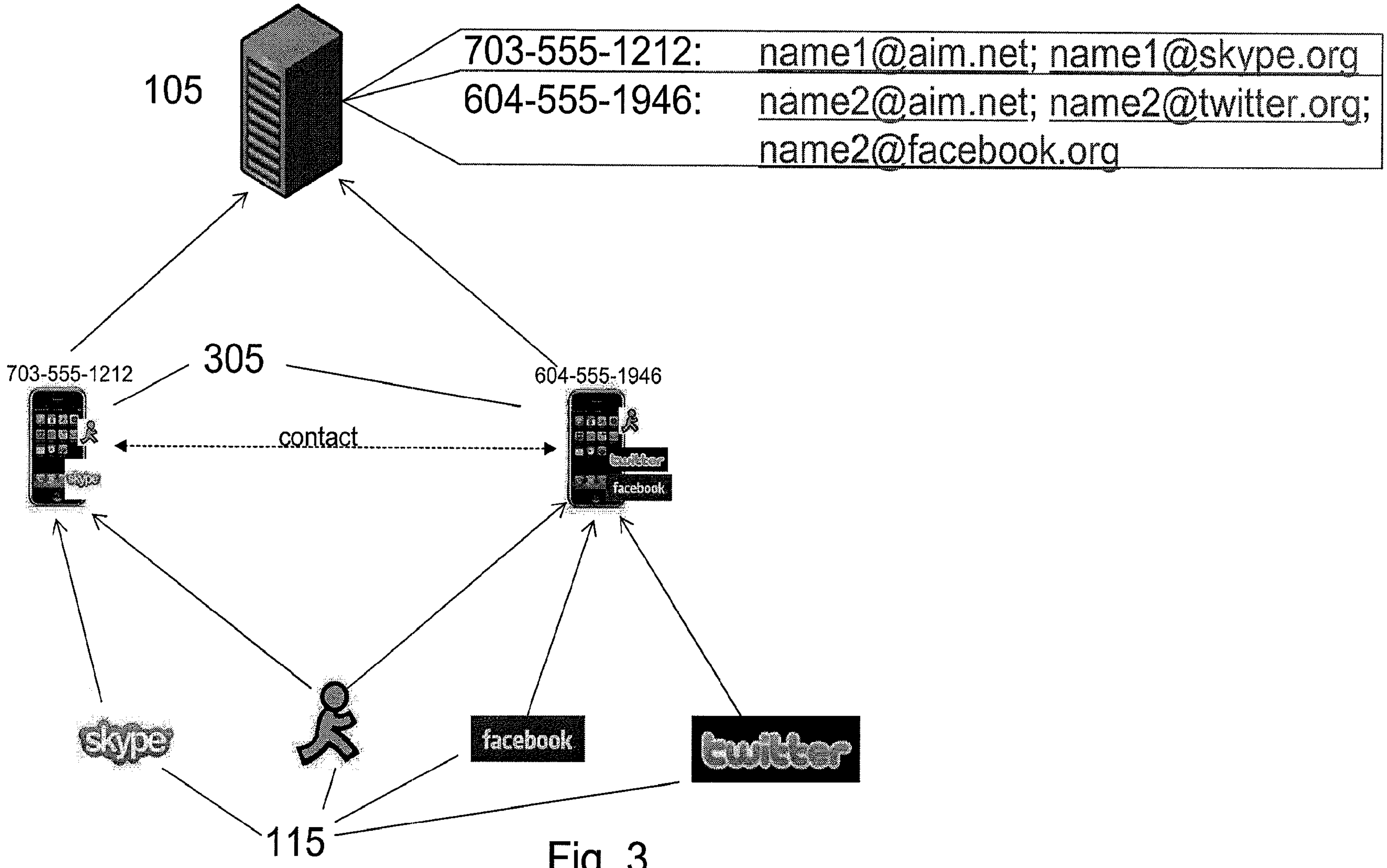

105
703-555-1212: name1@aim.net; name1@skype.org
604-555-1946: name2@aim.net; name2@twitter.org; name2@facebook.org
305
703-555-1212
604-555-1946
contact
skype
twitter
facebook
skype
facebook
twitter
115

Fig. 3

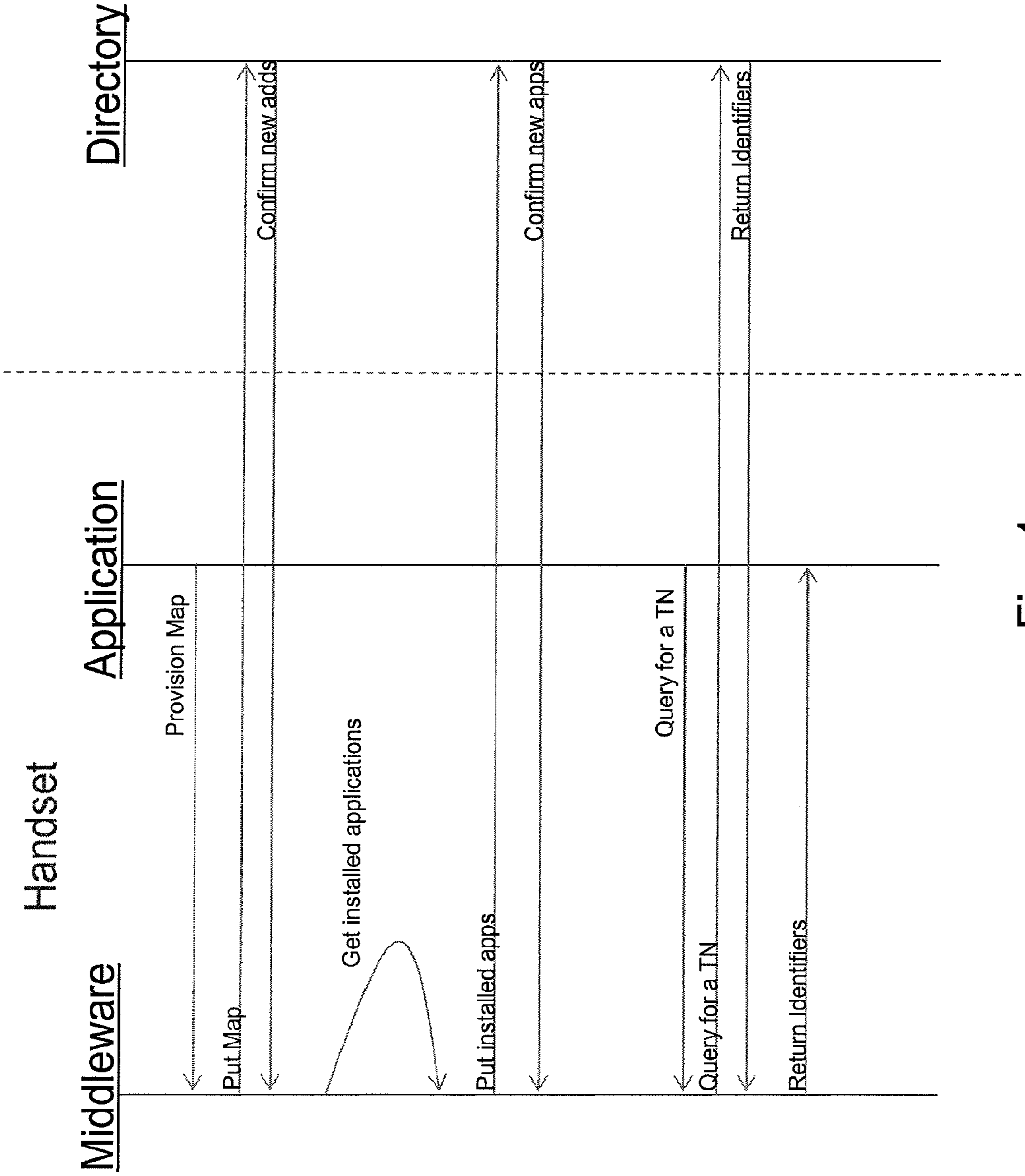

Middleware
Handset
Application
Directory
Provision Map
Put Map
Confirm new adds
Get installed applications
Put installed apps
Confirm new apps
Query for a TN
Query for a TN
Return Identifiers
Return Identifiers

Fig. 4

METHOD FOR DISTRIBUTING CONTACT INFORMATION BETWEEN APPLICATIONS

RELATED APPLICATIONS

This application is a Continuation of U.S. patent application Ser. No. 15/487,178, filed Apr. 13, 2017; which is a Continuation of U.S. patent application Ser. No. 12/705,268, filed Feb. 12, 2010, now U.S. Pat. No. 9,636,053, issued May 2, 2017. All of the aforementioned priority applications being hereby incorporated by reference in their respective entirety for all purposes.

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to the field of electronic communications. More particularly, the invention relates to sharing contact information across applications such as mobile telephones and the Internet.

Many existing technologies use ENUM or ENUM-like mechanisms for resolving telephone numbers into the URIs that identify network services. Many systems also enable portability of contact books, i.e., allowing a user to transfer a list of contacts from one computer to another, or synchronizing between mobile and desktop systems, or allowing a user to purchase a new mobile device and then to download or otherwise transfer a contact book from the old device. There are also conventional systems that use reciprocal authorization. For example, some instant messaging systems enable two parties to identify themselves as "buddies", who are then able to detect each other's presence, or online status, and to send messages to one another.

However, these conventional systems primarily address situations in which contact information is being transferred between devices controlled by a single user. In the instant messaging example, although two users are involved, reciprocal authorization is required, and the functionality is relatively limited. Accordingly, there is a need for a capability to share contact information between multiple users across applications simply and efficiently.

SUMMARY OF THE INVENTION

In one aspect, the invention provides a method for sharing contact information of a first user between a first application and a second application. The method comprises using a server on a computer network to perform the steps of: identifying first information relating to the first user; provisioning identification data associated with the first information; storing the provisioned data and the first information together in a first database; receiving a request for the provisioned data from a second user; determining whether the second user is authorized to obtain the provisioned data; when a determination is made that the second user is authorized to obtain the provisioned data, retrieving the provisioned data from the first database; and transmitting the provisioned data to a device associated with the second user.

The method may further comprise the step of receiving from the first user data for identifying authorized potential users. The step of determining whether the second user is authorized to obtain the provisioned data may further comprise determining whether the data for identifying authorized potential users includes data for identifying the second user. The step of identifying first information relating to the first user may further comprise receiving a prompt and the

first information from a device associated with the first user. The first information may comprise a telephone number. The device associated with the first user may comprise a mobile telephony device associated with the first user. The first information may comprise a telephone number associated with the device associated with the first user.

The mobile telephony device associated with the first user may comprise a middleware tool kit. The middleware tool kit may comprises a first network interface configured to transmit prompts and information over the computer network; a second network interface configured to transmit queries over the computer network and to receive responses to the transmitted queries; a first application programming interface (API) for receiving provisioning requests from applications; and a second API for receiving information requests from applications and for transmitting responses to the information requests to the requesting applications.

The provisioned data may comprise at least one Uniform Resource Indicator (URI). The at least one provisioned URI may be associated with an identifier selected from the group consisting of a telephone number, an e-mail address, an instant messaging handle, and a Uniform Resource Locator (URL) of a web page. The device associated with the second user may comprise a mobile telephony device associated with the second user. The step of transmitting the provisioned data may further comprise transmitting an SMS text message to the mobile telephony device associated with the second user. The step of provisioning identification data associated with the first information may further comprise transmitting an SMS text message to a device associated with the first user to determine whether the identification data to be provisioned is correctly associated with the first information.

In another aspect, the invention provides a system for sharing contact information of a first user between a first application and a second application. The system comprises a server configured for communicating with client devices over a computer network. The server is configured to perform the steps of: identifying first information relating to a first user; provisioning identification data associated with the first information; storing the provisioned data and the first information together in a first database; receiving a request for the provisioned data from a second user; determining whether the second user is authorized to obtain the provisioned data; when a determination is made that the second user is authorized to obtain the provisioned data, retrieving the provisioned data from the first database; and transmitting the provisioned data to a client device associated with the second user.

The server may be further configured to perform the steps of receiving from the first user data for identifying authorized potential users, and determining whether the data for identifying authorized potential users includes data for identifying the second user. The server may be further configured to perform the step of receiving a prompt and the first information from a client device associated with the first user. The first information may comprise a telephone number. The client device associated with the first user may comprise a mobile telephony device associated with the first user. The first information may comprise a telephone number associated with the client device associated with the first user.

The mobile telephony device associated with the first user may comprise a middleware tool kit. The middleware tool kit may comprise a first network interface configured to transmit prompts and information over the computer network; a second network interface configured to transmit queries over the computer network and to receive responses to the transmitted queries; a first application programming interface (API) for receiving provisioning requests from applications; and a second API for receiving information requests from applications and for transmitting responses to the information requests to the requesting applications.

The provisioned data may comprise at least one Uniform Resource Indicator (URI). The at least one provisioned URI may be associated with an identifier selected from the group consisting of a telephone number, an e-mail address, an instant messaging handle, and a Uniform Resource Locator (URL) of a web page. The client device associated with the second user may comprise a mobile telephony device associated with the second user. The server may be further configured to perform the step of transmitting an SMS text message to the mobile telephony device associated with the second user. The server may be further configured to perform the step of transmitting an SMS text message to a device associated with the first user to determine whether the identification data to be provisioned is correctly associated with the first information.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** illustrates a block diagram of an architecture for a system for sharing contacting information across applications according to a preferred embodiment of the invention.

FIG. **2** shows a flow chart that illustrates a method for sharing contacting information across applications according to a preferred embodiment of the invention.

FIG. **3** illustrates a directory containing installed applications and a database for storing provisioned contacting information as used in the system of FIG. **1**.

FIG. **4** illustrates an information flow diagram for the provisioning and querying steps of a method for sharing contacting information across applications according to a preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

The present inventors have recognized the need to enable sharing of contact information across multiple applications and among multiple users in a reasonably simple and efficient manner. Accordingly, it is an object of the present invention to provision ENUM in an automated and transparent way, while preventing public disclosure of contact information.

In a preferred embodiment of the invention, a system is designed to enable sharing of supplemental contact information between users of mobile telephones. When two mobile phone users know one another's telephone numbers, the system allows them to learn other ways of communicating over the Internet, for example email addresses or addresses for instant messaging. Applications can leverage this knowledge to help users discover contacts who also utilize the same application.

The invention was inspired by ENUM, in particular by the difficulty of seeding directories for translating telephone numbers into Internet identifiers. Many mobile telephones, notably the iPhone, have rich contact books with numerous identifiers that could be published via ENUM. The difficulties are that provisioning ENUM is typically a cumbersome step, and many users are reluctant to make their contact information public. Accordingly, in a preferred embodiment of the invention, the provisioning is made transparent, and reciprocal authorization whitelisting is used as a baseline, thereby preventing public disclosure of contact information.

Referring to FIG. **1**, a block diagram of an architecture of a system **100** according to a preferred embodiment of the invention is shown. The system **100** includes a directory **105** and a middleware toolkit **110** which are leveraged by applications **115** to discover new identifiers associated with the telephone number of a contact. The system **100** also includes an authorization database **120** which can be accessed by the directory **105** in order to verify that a requesting client is authorized to receive contacting information in response to a request for same. In a broad sense, the system **100** is designed to translate one identifier into a set of different identifiers. The identifier so translated is, for the sake of readability, hereafter exemplified by a telephone number, and although the telephone number is used for the translated identifier in the preferred implementation, the invention is not limited to the use of telephone numbers for translated identifiers.

Referring to FIG. **2**, a flow chart **200** that illustrates a method of sharing contacting information across applications according to preferred embodiment of the present invention is shown. In the first step **205**, the identifiers associated with a telephone number are provisioned into a server on a computer network, either as a bulk operation or one by one, by various clients attached to the same computer network. In the second step **210**, upon receiving the provisioning instructions from clients, the server stores that data in a database table, with the telephone number serving as the key and one or more identifiers associated with the telephone number serving as the value. In the third step **215**, a translation is instigated by one such client, generally in order to acquire information provisioned by other clients, and performed by said server, which returns the response to the client.

In the fourth step **220**, the server verifies that the requesting client is authorized to receive the requested information by consulting a second database, which includes information that identifies authorized senders of queries. The second database may be resident locally, or it may reside elsewhere on the network. Then, upon verification that the requesting client is so authorized, the server returns the identifiers in response to the client, and the client delivers the response to an application in step **225**. Finally, in step **230**, the application may make use of the identifiers immediately, or it may store them for future use or invocation by the user. If the identifiers are stored, they are stored for a specific lifetime, after which application must ask the client to make a new query to the server.

In the system **100**, an application may learn identifiers of a user through manual input, as is the case with a contact book, or the application may actually assign identifiers to a use, as is the case with an instant messaging application in which a user registers a new identifier. The system **100** may be implemented, for example, where users commonly contact one another by dialing a telephone number, and where terminals commonly record the calling and called parties in a telephone conversation, thus building a list of contacts by telephone number. In this manner, the system **100** allows users to discover other communications and applications identifiers associated with their contacts, even if they know their contact only by telephone number.

Referring again to FIG. **1**, the directory **105** is the back-end database that maintains the mappings from telephone numbers to various application identifiers, and also the server interface to that directory. The directory **105** is populated by the middleware toolkit **110**, which sends provisioning information to the directory **105**. The directory **105** is queried through the middleware toolkit **110** by applications **115** that want to acquire mappings for a particular telephone number. The directory **105** also maintains, or accesses externally, a list of contacts associated with a particular telephone number, in order to learn which telephone numbers are authorized to query for a particular application.

The middleware toolkit **110** is a software library that contains the necessary code to interface with the directory **105** over the Internet. Applications **115** use the middleware toolkit **110** to learn about the application identifiers associated with a particular telephone number. The application **115** is a communications application residing on a general purpose computer, be it a desktop or a mobile handset, that makes use of the middleware toolkit to learn and provision the application identifiers associated with a telephone number. The application **115** may be understood broadly to include any software used for personal communication on the Internet, including various messaging, real-time audio transmission, and gaming applications.

An identifier includes any information that represents a user within the scope of a particular communications system. Examples include telephone numbers, e-mail addresses, instant messaging handles, and the Uniform Resource Locator (URL) of a web page where a user might be reached. Calling, invoking, or dereferencing an application identifier typically causes the invocation of the application and contacts through the application the user has designated by the identifier.

The directory **105** resides on one or more servers. The server is preferably implemented by the use of one or more general purpose computers, such as, for example, a SUN MICROSYSTEMS FIRE F 15K. Each of the middleware tool kit **110**, the applications **115**, and the authorization database **120** may also be implemented by the use of one or more general purpose computers, such as, for example, a typical personal computer manufactured by DELL, GATEWAY, or HEWLETT-PACKARD; or more preferably, the middleware tool kit **110** and the applications **115** may be implemented on a smart mobile telephone, such as, for example, an APPLE IPHONE or a BLACKBERRY STORM mobile telephone or a smart mobile telephone manufactured by. Each of the server and the client devices on which the middleware tool kit **110**, the applications **115**, and the authorization database **120** reside can include a microprocessor. The microprocessor can be any type of processor, such as, for example, any type of general purpose microprocessor or microcontroller, a digital signal processing (DSP) processor, an application-specific integrated circuit (ASIC), a programmable read-only memory (PROM), or the like. The server may use its microprocessor to read a computer-readable medium containing software that includes instructions for carrying out one or more of the functions of the directory **105**, as further described below.

Each of the server and the client devices on which the middleware tool kit **110**, the applications **115**, and the authorization database **120** reside can also include computer memory, such as, for example, random-access memory (RAM). However, the computer memory of each of the server and the client devices can be any type of computer memory or any other type of electronic storage medium that is located either internally or externally to the server or the client devices, such as, for example, read-only memory (ROM), compact disc read-only memory (CDROM), electro-optical memory, magneto-optical memory, an erasable programmable read-only memory (EPROM), an electrically-erasable programmable read-only memory (EEPROM), a computer-readable medium, or the like. According to exemplary embodiments, the respective RAM can contain, for example, the operating program for either the server or the respective client device. As will be appreciated based on the following description, the RAM can, for example, be programmed using conventional techniques known to those having ordinary skill in the art of computer programming. The actual source code or object code for carrying out the steps of, for example, a computer program can be stored in the RAM. Each of the server and the client devices can also include a database. The database can be any type of computer database for storing, maintaining, and allowing access to electronic information stored therein. The server preferably resides on a network, such as a local area network (LAN), a wide area network (WAN), a virtual private network (VPN), or the Internet. Each of the client devices preferably is wirelessly connected to the network on which the host server resides, thus enabling electronic communications between the server and the respective client device.

In a preferred embodiment, the directory **105** includes the following components:

a back-end database whose keys are telephone numbers and whose values are identifiers of applications, for example, e-mail addresses, running on a general purpose computer

a first network interface that receives queries and sends responses to those queries after consulting the database

a second network interface that receives provisioning from middleware toolkits to populate the database

a set of policies for the formulation of responses, based on the preference of users, which are either defaults built into the system or are provisioned directly by the user through a third network interface

In a preferred embodiment, the middleware toolkit **110** includes the following components:

a first network interface for sending provisioning requests to the directory

a second network interface for sending queries to the directory and receiving responses

a first application programming interface (API) for receiving provisioning requests from applications

a second application programming interface for receiving requests for the identifiers associated with a telephone number, and sending responses back to the application

The system **100** may be implemented by installing the middleware **110** in a mobile telephone device, where one or more applications **115**, such as, for example, a contact book, invoke the middleware toolkit **110**. The middleware toolkit **110** communicates over the Internet with the directory **105**, either by provisioning the directory **105**, or querying for information that has already been provisioned in the directory **105**, or both. The application **115** then makes use of the contact information learned by the middleware toolkit **110**; the manner in which this information is used by the application **115** varies based on the application's needs. For example, a contact book application could render to the user the various contact addresses associated with applications that it learned from the middleware toolkit **110**. The user might then select one of these contact addresses in order to initiate a communication with that application, for example, e-mail.

Referring to FIG. **3**, in a preferred embodiment of the invention, mobile Internet-enabled smart telephones **305** are typically used by clients of the system **100**. The telephones **305** are understood to be general purpose end user devices which have been assigned telephone numbers; for example, the Apple iPhone. The middleware toolkit **110** is incorporated into one or more applications **115** running on the mobile telephone **305**, and each of these applications could register an associated communications address with the directory **105**.

Referring to FIG. **4**, in a preferred embodiment of the present invention, the directory **105** receives queries and sends responses using a protocol such as ENUM, which is a DNS-based protocol for the mapping of telephone numbers into Uniform Resource Indicators (URIs), which are the identifiers that designate Internet applications such as web pages and e-mail inboxes. The middleware toolbox **110** therefore acts as an ENUM resolver, a type of DNS resolver with additional capabilities to understand NAPTR DNS Resource Records, which contain URIs, and is capable of properly formulating ENUM queries and understanding ENUM replies. The directory **105** is capable of mapping ENUM queries to the keys of its database, extracting the values associated with those keys, and formulating them into NAPTR DNS RR format to be sent back to the client.

One exemplary application **115** that could make use of the URIs returned by the directory **105** is an extension to the iPhone contact book. A user might provision, through the user interface of the iPhone, certain identifiers associated with his own telephone number. The contact book application uploads these identifiers to the directory, along with the list of contacts and associated telephone numbers that the user has provisioned in his contact book. Whenever any of those contacts queries the directory **105** for the user's telephone number, the directory **105** will return the set of provisioned identifiers, which will in turn populate the querying user's entry for the provisioning user in his own contact book. This allows identifiers to spread automatically and seamlessly between contacts, without revealing that information to anyone who is not a contact.

In an alternative embodiment, the system **100** may be implemented by devices that are not tied to mobile telephones, but are identified by telephone numbers. This could include, for example, telephony applications operating on a desktop computer. This could also include applications that run on a general purpose computer operated by a user who also subscribes to a traditional, non-Internet based telephone service, and wishes simply to use that telephone number as a means of identifying various Internet services.

Some external applications might benefit from querying the database to learn which telephone numbers are associated with various applications. For example, a "lobby service" that helps users find partners for online games might query the database externally to learn which games two users have in common as part of a rendezvous activity.

The use of reciprocal authorization works according to the following rule: If a first user has provisioned a second user as a contact, then the second user is authorized to see the identifiers provisioned by the first user, and conversely if the second user has provisioned the first user as a contact, then the first user is authorized to see the identifiers provisioned by the second user. Reciprocal authorization is a simple policy. However, users may desire finer grained policy controls that could, for example, allow particular identifiers to be authorized or forbidden to particular requestors on a case-by-case basis. In a preferred embodiment of the invention, the system may use any acceptable form of authorization, including fine-grained policy controls that make authorization determinations on a case-by-case basis.

While the present invention has been described with respect to what is presently considered to be the preferred embodiment, it is to be understood that the invention is not limited to the disclosed embodiments. To the contrary, the invention is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims. The scope of the following claims is to be accorded the broadest interpretation so as to encompass all such modifications and equivalent structures and functions.

What is claimed is:

1. A method for sharing contact information of a first user between a first application and a second application associated with a second user, the method comprising using a server on a computer network to perform steps of:

identifying a first identifier relating to the first user;

provisioning contact information associated with the first identifier, wherein the contact information includes a set of different identifiers, each of which is different from the first identifier;

storing the contact information and the first identifier together in a first database;

receiving a request for the contact information from the second user, wherein a second identifier is associated with the second user;

determining whether the second user is authorized to obtain the contact information, based on the second identifier being in a set of authorized identifiers authorized to access the contact information;

when a determination is made that the second user is authorized to obtain the contact information, retrieving the contact information from the first database; and

transmitting the contact information to the second application associated with the second user without receiving an authorization signal from the first user in response to the request.

2. The method of claim **1**, further comprising:

storing, in a server memory of the server, a mapping of the first identifier to the contact information for the first user and the set of authorized identifiers authorized to access the contact information.

3. The method of claim **2**, wherein each of the set of authorized identifiers authorized to access the contact information is an access key to the contact information in the server memory.

4. The method of claim **1**, wherein a mobile device is associated with the second user, and the mobile device includes a middleware application having a first application programming interface (API) and a second API, the method further comprising:

receiving, via the first API, requests for contact information from applications and transferring, via the first API, responses to the requests to the applications; and

transmitting, via the second API, the requests for contact information to the server over the network and receiving, via the second API, the responses to the requests from the server.

5. The method of claim **1**, wherein the contact information for the first user includes at least one Uniform Resource Indicator (URI).

6. The method of claim **5**, wherein the at least one URI is associated with an identifier selected from a group consisting of an e-mail address, an instant messaging handle, and a Uniform Resource Locator (URL) of a web page.

7. The method of claim **1**, wherein transmitting the contact information comprises transmitting an SMS text message to the second application.

8. A network server for sharing contact information of a first user between a first application and a second application associated with a second user, comprising:

one or more processors; and one or more memory resources storing instructions that, when executed by the one or more processors, cause the network server to perform operations including: identifying a first identifier relating to the first user;

provisioning contact information associated with the first identifier, wherein the contact information includes a set of different identifiers, each of which is different from the first identifier;

storing the contact information and the first identifier together in a first database; receiving a request for the contact information from the second user, wherein a second identifier is associated with the second user;

determining whether the second user is authorized to obtain the contact information, based on the second identifier being in a set of authorized identifiers authorized to access the contact information;

when a determination is made that the second user is authorized to obtain the contact information, retrieving the contact information from the first database; and

transmitting the contact information to the second application associated with the second user without receiving an authorization signal from the first user in response to the request.

9. The network server of claim **8**, further comprising instructions to perform operations for:

storing, in a server memory of the network server, a mapping of the first identifier to the contact information for the first user and the set of authorized identifiers authorized to access the contact information.

10. The network server of claim **9**, wherein each of the set of authorized identifiers authorized to access the contact information is an access key to the contact information in the server memory.

11. The network server of claim **8**, wherein the network server is configured to communicate with a mobile device associated with the second user, the mobile device including a middleware application that comprises:

a first application programming interface (API) for receiving requests for account identifiers from applications and transferring responses to the requests to the applications; and

a second API for transmitting the requests for account identifiers to the network server over the network and receiving the responses to the requests from the network server.

12. The network server of claim **8**, wherein the contact information for the first user includes at least one Uniform Resource Indicator (URI).

13. The network server of claim **12**, wherein the at least one URI is associated with an identifier selected from a group consisting of an e-mail address, an instant messaging handle, and a Uniform Resource Locator (URL) of a web page.

14. The network server of claim **8**, wherein the transmitting the contact information comprises transmitting an SMS text message to the second application.

15. A non-transitory computer-readable medium that stores instructions, executable by one or more processors of a network server for sharing contact information of a first user between a first application and a second application associated with a second user, to cause the one or more processors to perform operations that comprise:

identifying a first identifier relating to the first user; provisioning contact information associated with the first identifier, wherein the contact information includes a set of different identifiers, each of which is different from the first identifier;

storing the contact information and the first identifier together in a first database;

receiving a request for the contact information from the second user, wherein a second identifier is associated with the second user;

determining whether the second user is authorized to obtain the contact information, based on the second identifier being in a set of authorized identifiers authorized to access the contact information;

when a determination is made that the second user is authorized to obtain the contact information, retrieving the contact information from the first database; and

transmitting the contact information to the second application associated with the second user without receiving an authorization signal from the first user in response to the request.

16. The non-transitory computer-readable medium of claim **15**, storing further instructions to perform operations that comprise:

storing, in a server memory of the network server, a mapping of the first identifier to the contact information for the first user and the set of authorized identifiers authorized to access the contact information.

17. The non-transitory computer-readable medium of claim **16**, wherein each of the set of authorized identifiers authorized to access the contact information is an access key to the contact information in the server memory.

18. The non-transitory computer-readable medium of claim **15**, wherein the contact information for the first user includes at least one Uniform Resource Indicator (URI).

19. The non-transitory computer-readable medium of claim **18**, wherein the at least one URI is associated with an identifier selected from a group consisting of an e-mail address, an instant messaging handle, and a Uniform Resource Locator (URL) of a web page.

20. The non-transitory computer-readable medium of claim **15**, wherein the transmitting the contact information comprises transmitting an SMS text message to the second application.

* * * * *

Exhibit 6

US010547739B2

(12) **United States Patent**
Cody et al.

(10) **Patent No.: US 10,547,739 B2**
(45) **Date of Patent: *Jan. 28, 2020**

(54) **COMPUTING DEVICE AND SYSTEM FOR RENDERING CONTACT INFORMATION THAT IS RETRIEVED FROM A NETWORK SERVICE**

(71) Applicant: **Neustar, Inc.**, San Francisco, CA (US)

(72) Inventors: **Tim Cody**, Sterling, VA (US); **Guido Jonjie S. Sena, Jr.**, Sterling, VA (US); **Ken Politz**, Sterling, VA (US); **John Devolites**, Sterling, VA (US); **Michael Cooley**, Sterling, VA (US)

(73) Assignee: **Neustar, Inc.**, Sterling, VA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/949,944**

(22) Filed: **Apr. 10, 2018**

(65) **Prior Publication Data**

US 2018/0338039 A1 Nov. 22, 2018

Related U.S. Application Data

(63) Continuation of application No. 15/295,994, filed on Oct. 17, 2016, now Pat. No. 9,955,003.

(60) Provisional application No. 62/242,851, filed on Oct. 16, 2015.

(51) **Int. Cl.**

H04M 3/42	(2006.01)
H04M 1/57	(2006.01)
H04M 1/663	(2006.01)
H04M 1/725	(2006.01)
H04M 3/493	(2006.01)

(52) **U.S. Cl.**
CPC ***H04M 3/42059*** (2013.01); ***H04M 1/575*** (2013.01); ***H04M 3/42042*** (2013.01); *H04M 1/663* (2013.01); *H04M 1/72547* (2013.01); *H04M 3/4931* (2013.01); *H04M 2203/354* (2013.01)

(58) **Field of Classification Search**
CPC H04W 4/02; H04W 12/12; H04W 64/006; H04W 8/005; H04M 1/72569; H04M 1/72572; H04M 3/42161
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

9,955,003	B2 *	4/2018	Cody	.... H04M 3/42059
2008/0045234	A1 *	2/2008	Reed	.... H04W 8/02 455/456.1
2014/0338006	A1 *	11/2014	Grkov	.... H04L 63/14 726/35
2018/0206124	A1 *	7/2018	Mahaffey	.... G06F 21/88

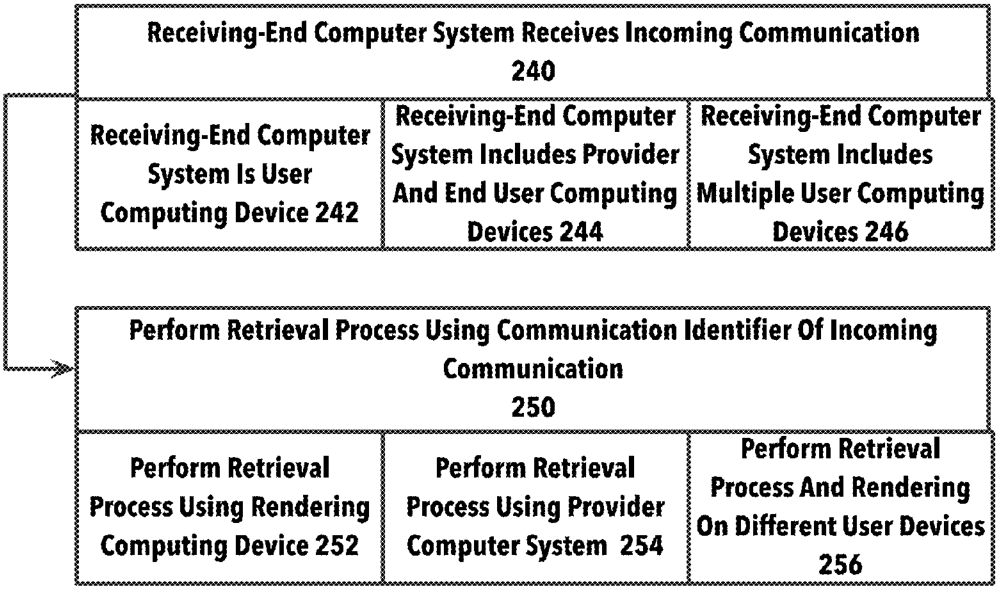
* cited by examiner

Primary Examiner — Diane D Mizrahi
(74) *Attorney, Agent, or Firm* — Sterne, Kessler, Goldstein & Fox P.L.L.C.

(57) **ABSTRACT**

A contact information system provides an independent network authority for providing contact information in connection with incoming calls or messages. The contact information system utilizes a database of communication identifiers to provide contact information for end user devices that receive incoming communications which specify communication identifiers that are stored in the database.

13 Claims, 5 Drawing Sheets


Receiving-End Computer System Receives Incoming Communication
240
Receiving-End Computer System Is User Computing Device 242
Receiving-End Computer System Includes Provider And End User Computing Devices 244
Receiving-End Computer System Includes Multiple User Computing Devices 246
Perform Retrieval Process Using Communication Identifier Of Incoming Communication
250
Perform Retrieval Process Using Rendering Computing Device 252
Perform Retrieval Process Using Provider Computer System 254
Perform Retrieval Process And Rendering On Different User Devices
256

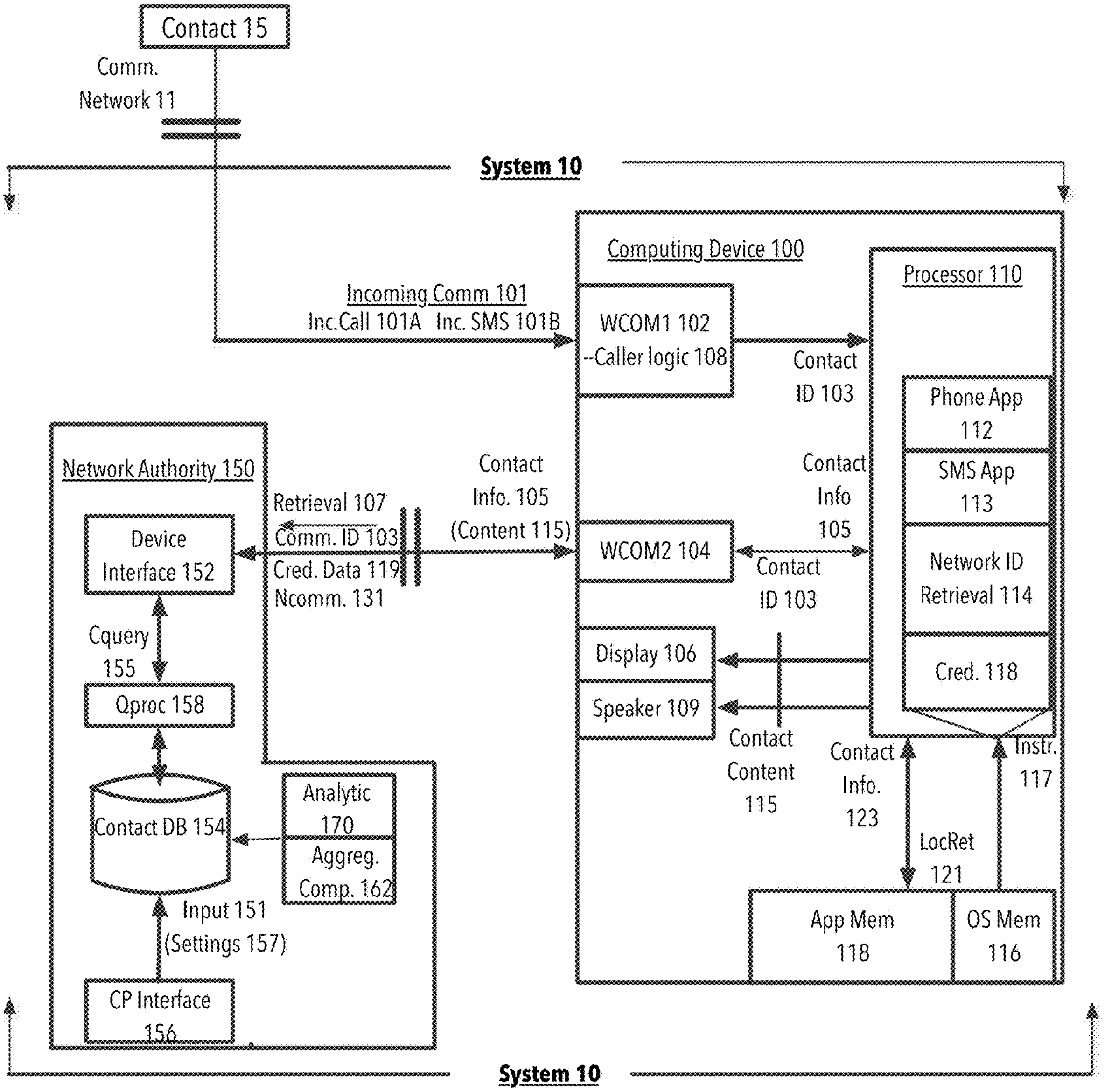

Contact 15
Comm.
Network 11
System 10
Computing Device 100
Processor 110
Incoming Comm 101
Inc.Call 101A Inc. SMS 101B
WCOM1 102
--Caller logic 108
Contact
ID 103
Phone App
112
SMS App
113
Network ID
Retrieval 114
Cred. 118
Network Authority 150
Device
Interface 152
Retrieval 107
Comm. ID 103
Cred. Data 119
Ncomm. 131
Contact
Info. 105
(Content 115)
WCOM2 104
Contact
Info
105
Contact
ID 103
Cquery
155
Qproc 158
Display 106
Speaker 109
Contact
Content
115
Contact
Info.
123
Instr.
117
LocRet
121
Contact DB 154
Analytic
170
Aggreg.
Comp. 162
Input 151
(Settings 157)
App Mem
118
OS Mem
116
CP Interface
156
System 10

FIG. 1

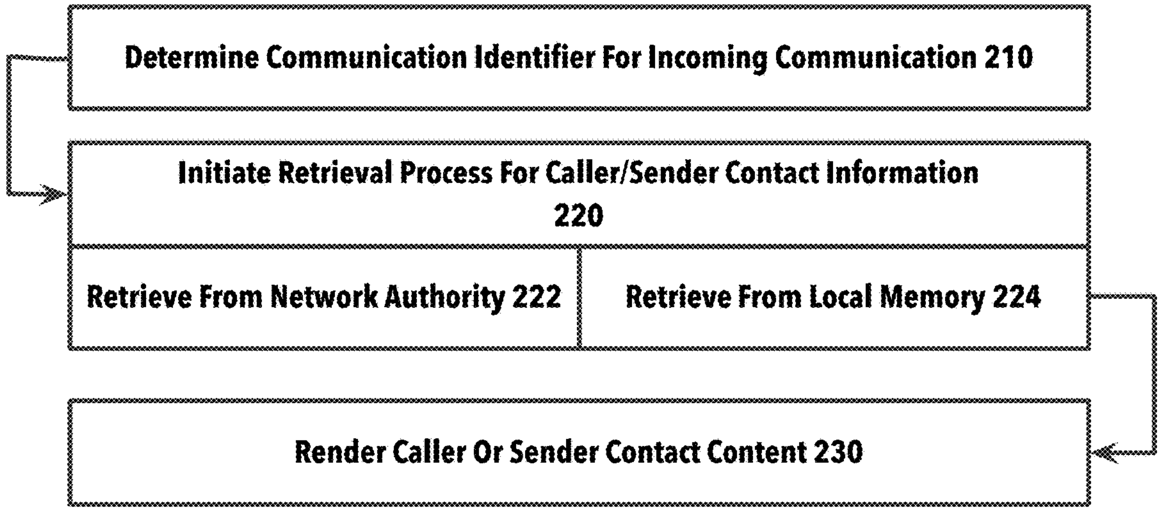

Determine Communication Identifier For Incoming Communication 210
Initiate Retrieval Process For Caller/Sender Contact Information 220
Retrieve From Network Authority 222
Retrieve From Local Memory 224
Render Caller Or Sender Contact Content 230

FIG. 2A

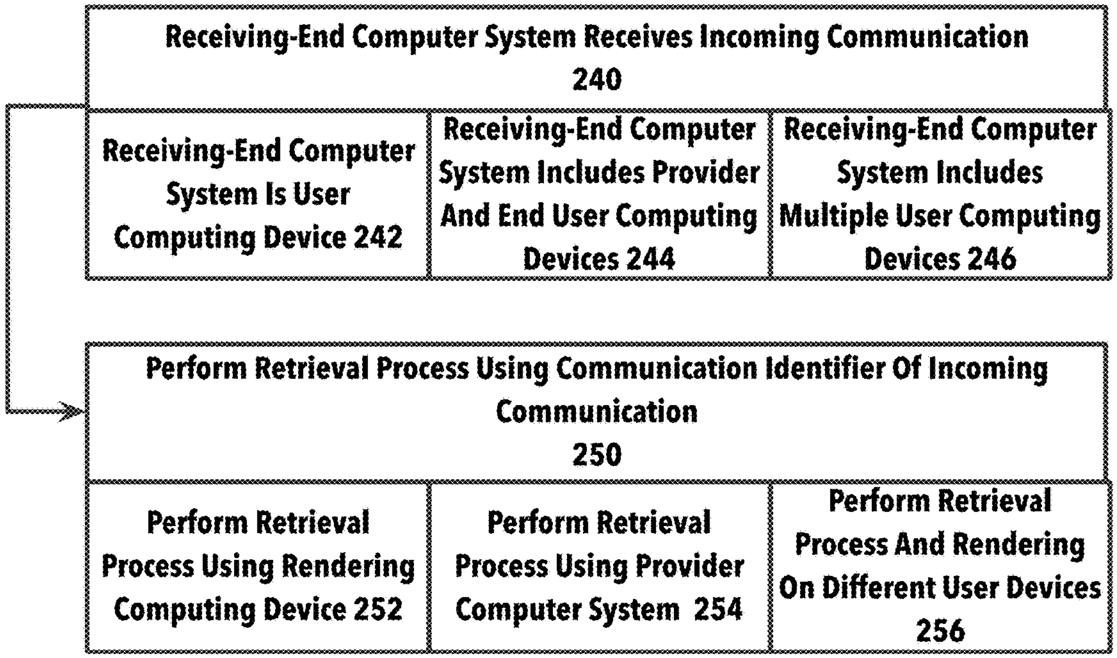

Receiving-End Computer System Receives Incoming Communication 240
Receiving-End Computer System Is User Computing Device 242
Receiving-End Computer System Includes Provider And End User Computing Devices 244
Receiving-End Computer System Includes Multiple User Computing Devices 246
Perform Retrieval Process Using Communication Identifier Of Incoming Communication 250
Perform Retrieval Process Using Rendering Computing Device 252
Perform Retrieval Process Using Provider Computer System 254
Perform Retrieval Process And Rendering On Different User Devices 256

FIG. 2B

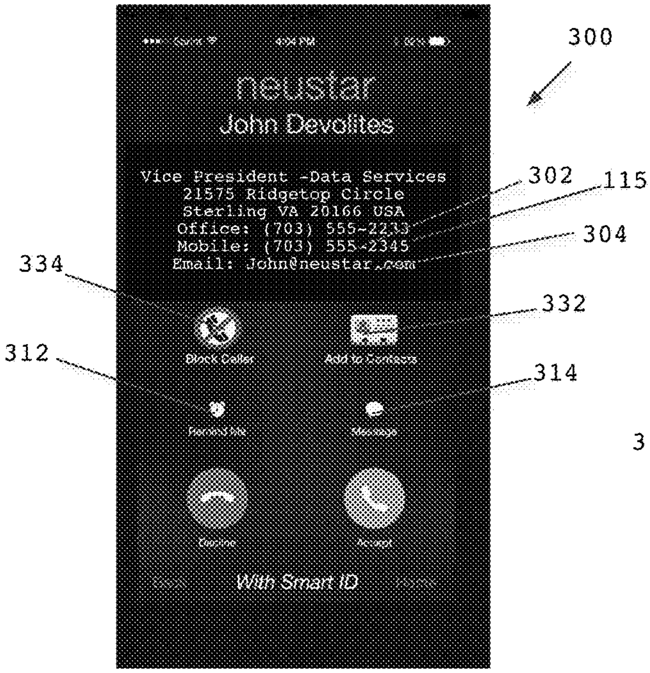


FIG. 3A

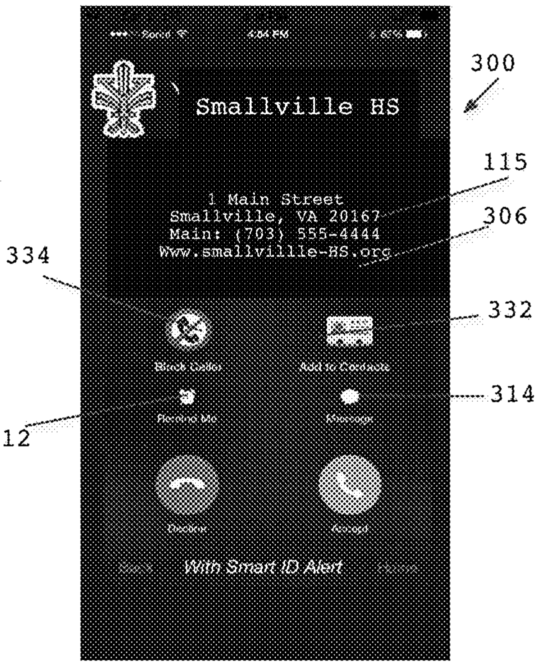


FIG. 3B

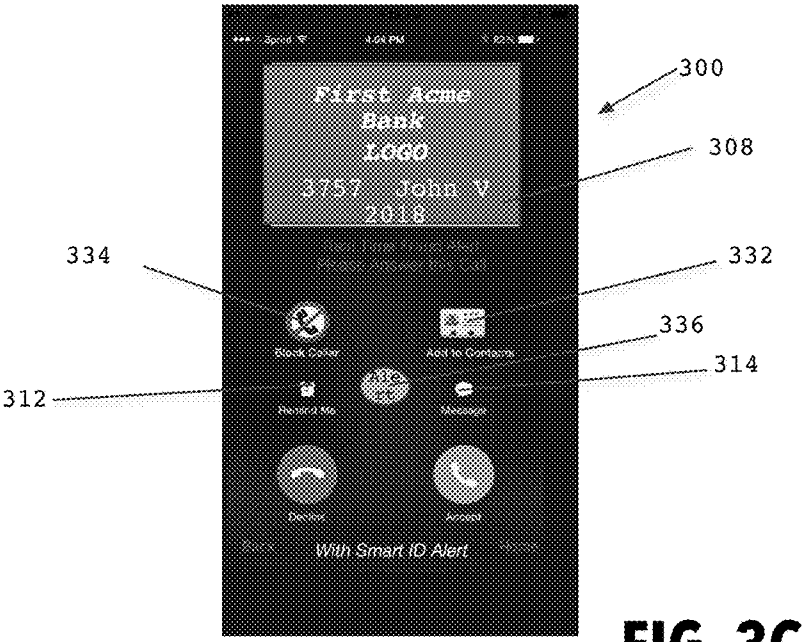


FIG. 3C

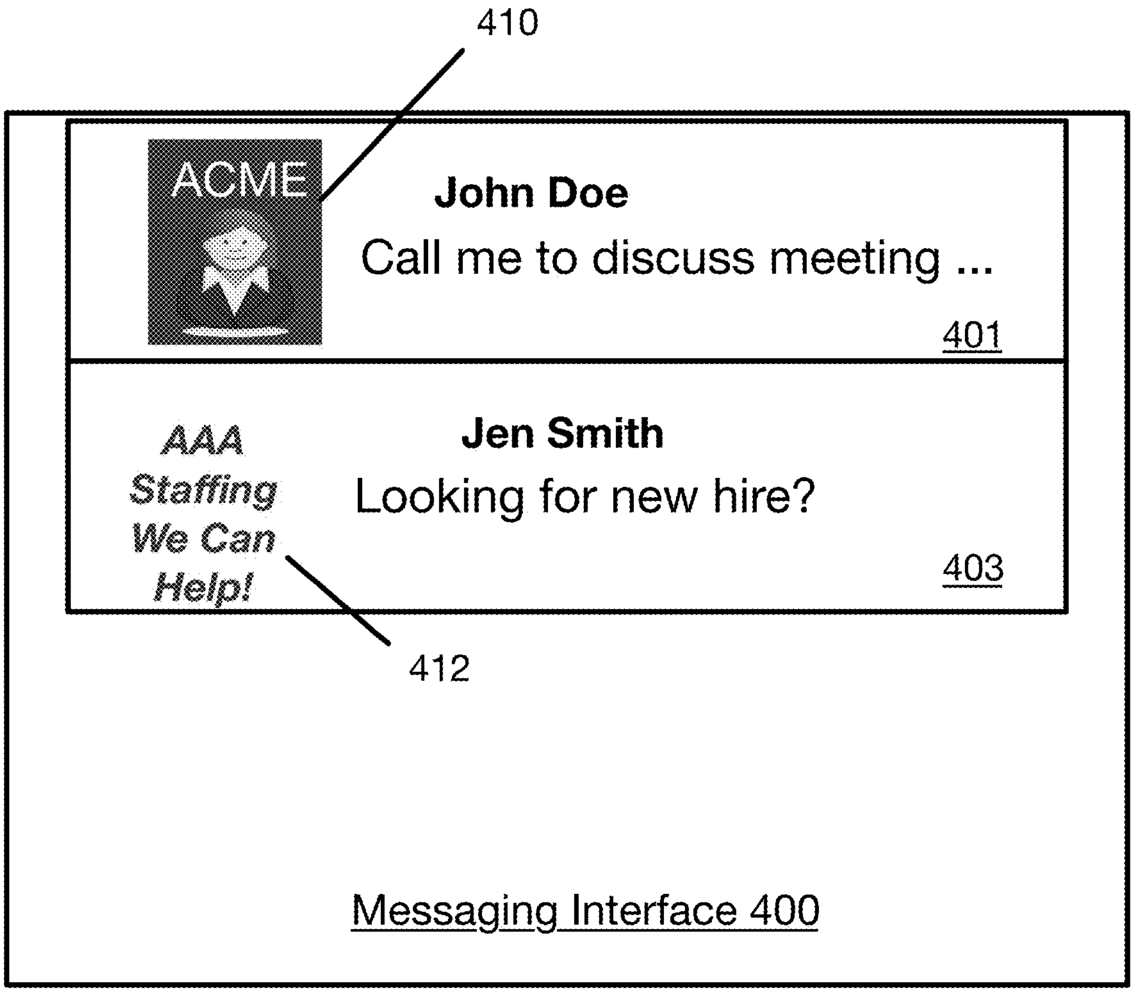

410
ACME
John Doe
Call me to discuss meeting ...
401
AAA Staffing We Can Help!
Jen Smith
Looking for new hire?
403
412
Messaging Interface 400

FIG. 4

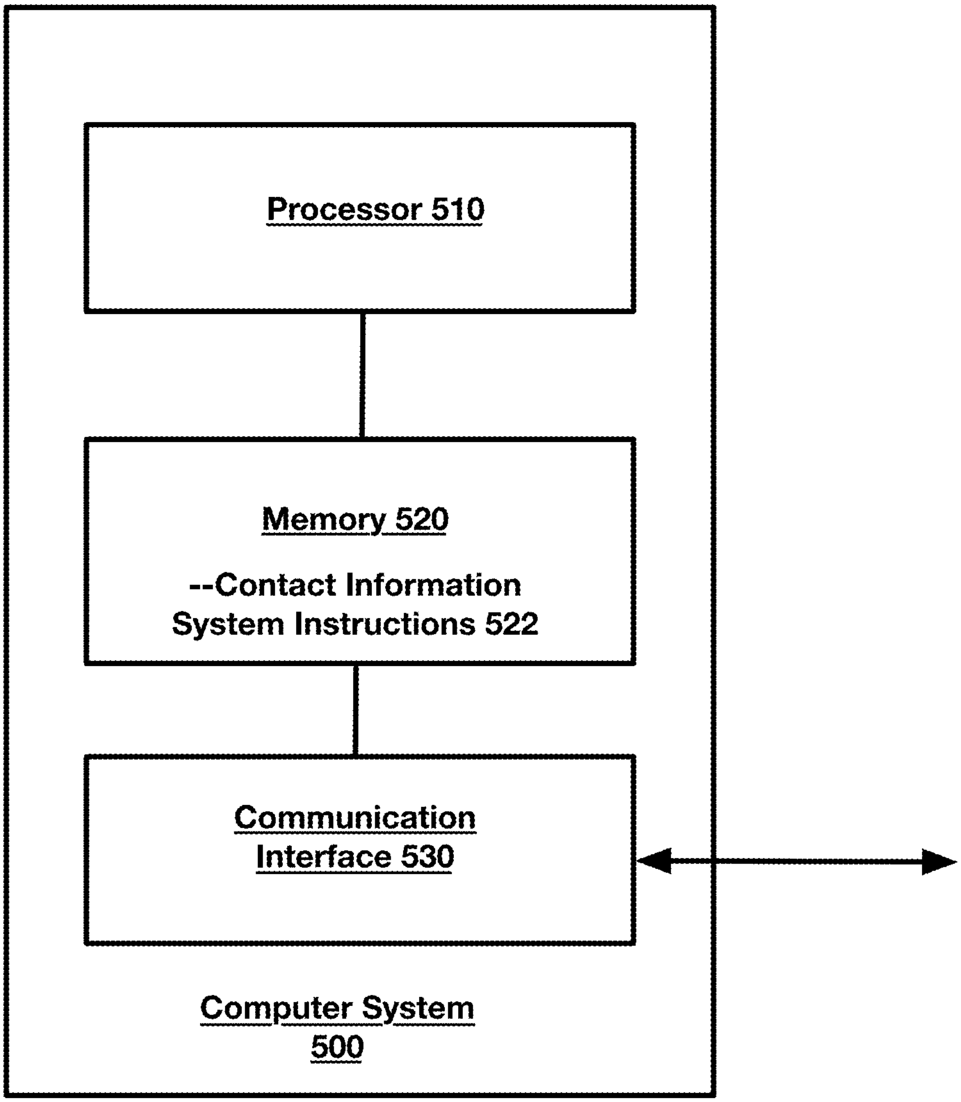

Processor 510
Memory 520
--Contact Information
System Instructions 522
Communication
Interface 530
Computer System
500

FIG. 5

COMPUTING DEVICE AND SYSTEM FOR RENDERING CONTACT INFORMATION THAT IS RETRIEVED FROM A NETWORK SERVICE

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a Continuation of U.S. patent application Ser. No. 15/295,994, filed Oct. 17, 2016; which claims benefit of priority to Provisional U.S. Patent Application No. 62/242,851, filed on Oct. 16, 2015; the aforementioned priority applications being hereby incorporated by reference in their respective entirety for all purposes.

BACKGROUND

Caller identification, or "caller id" is a telephonic service that has been present for a number of years. Prior to network-enabled telephonic devices, such services used the Public Switch Telephone Network ("PSTN") to deliver the caller information at the time the call was received. With the advance of mobile telephony devices in particular, caller information has increasingly been displayed via locally stored contact information.

Conventional approaches also exist where the caller information is inserted as additional data accompanying an incoming call at a network node associated with the receiving device. For example, cellular carriers and service providers have previously inserted caller information into the data stream of an incoming call.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** illustrates a computing device and system for rendering caller information from an authoritative caller information service, according to one or more examples.

FIG. **2**A illustrates an example method for providing a contact information service, according to one or more examples.

FIG. **2**B illustrates an example method for implementing a contact information service on a distributed computing environment of an end user.

FIG. **3**A through FIG. **3**C illustrate variations of a phone application interface for displaying caller information provided from a caller information system, according to one or more examples.

FIG. **4** illustrates an example message interface for displaying sender contact information provided from a contact information system, according to one or more examples.

FIG. **5** illustrates a computer system on which a caller information system may be implemented.

DETAILED DESCRIPTION

Examples described include a computing device that operates to perform a retrieval process in which an operating system component retrieves contact information associated with an incoming communication. According to some examples, the incoming communication may specify a phone number as a communication identifier. By way of further example, the incoming communication may correspond to an incoming call connect, Multimedia Message Service message (MMS) Short Message Service message (SMS), communicated over one or more of a public, cellular network or Internet Protocol ("IP") communication medium.

Still further, in some examples, a contact information system is provided to provide an independent network authority for contact information. The system may include one or more computers that utilize a database of phone numbers in providing contact information to end user devices that receive incoming communications which utilize phone numbers stored in the database.

According to some examples, one or more computers implement an independent network authority by providing a contact party interface to enable a plurality of entities that are each an authorized user of a corresponding phone number, to specify contact information to render on end user devices when end user devices receive incoming communications from that entity's phone number. The one or more computers further implement the network authority by fielding retrieval requests from a plurality of end user devices, in which each of the plurality of end user devices generate a retrieval request that specifies a phone number of an incoming communication received on that device. For each retrieval request, the one or more computers identify, from the database, contact information associated with the phone number of the retrieval request. The one or more computers transmit the contact information to the end user device that generated the retrieval request.

According to some examples, a computing device is enabled to use a network communication medium, separate from a telephony network and/or channel on which the incoming call is received ("PSTN" or cellular voice channel), in order to retrieve caller information (e.g., "Caller ID") from an independent authority where such information is stored and validated.

Among other benefits, contact information can be rendered on a computing device, in connection with an incoming communication (e.g., incoming call, incoming, new SMS message or new MMS message) subject to rules and/or legal requirements of the independent network authority where such information is stored. In this respect, information for a contact that initiates the communication can be ensured as being valid and authentic, in that the information rendered on the computing device originates from the network authority.

In some variations, a computing device is enabled to retrieve sender contact information from an independent network authority, to render in connection with a newly received message. The sender contact information may be trusted as identifying the sender, as it is provided from the independent network authority. The newly received message may correspond to a message communicated under, for example, a Short Message Service ("SMS"), Multimedia Media Message ("MMS"), or message communicated using an alternative messaging transport. The computing device may retrieve and render the contact information to display as part of the message header when the message is listed as an item in a messaging box or folder of the computing device. As an addition or alternative, the sender contact information may be displayed with a rendered a portion of the message in an open state.

As described with various examples, the network authority can implement a caller and/or sender contact information service that (i) enables the service to access and use validated information about entities whom are associated with phone numbers or other communication identifiers, and (ii) complies with rules and/or laws that ensure the contact information provided through the service is valid and authentic.

In some examples, the contact information service implemented through the network service can operate in connection with operating system level functionality of computing devices which receive incoming calls. In this regard, some examples include a contact information platform for use with devices that receive incoming calls and messages. In some variations, the contact information platform may include or operate with a network retrieval component that is implement as an operating system level component of a computing device. In other variations, the network retrieval component may be implemented as an application or application level component. On a computing device, the network retrieval component performs a network retrieval function to access the contact information service when an incoming call or message is received.

When implemented as an operating system level component, the network retrieval component can provide additional security to prevent, for example, other third-party providers (e.g., cellular carries) from circumventing the independent network authority, while providing a similar service. Thus, for example, a caller may not be able to avoid having its caller information displayed on a computing device when the caller initiates a phone call using an associated phone number. Depending on implementation, the caller contact information (or sender contact information) can identify the caller (or sender) name (e.g., corporation, individual, organization), caller contact information (e.g., phone number being used for call or message, alternative phone number, email address or messaging handle), or caller/sender contact category (e.g., "solicitation", "important" "residential" etc.). Still further, the caller or sender contact information can be rich, such as provided through formatted text data, image, and other media. In some variations, the caller or sender contact information can also include, or be transformed on the receiver device, to include functional data items that trigger automated and/or programmatic actions.

According to some examples, a computing device can be configured with operating system level functionality to cause the computing device to access the network authority when an incoming call is received. In variations, the computing device can perform a multi-step retrieval process which includes first checking a local or trusted user-specific data store (e.g., contact records stored on device) in order to determine whether caller information exists for the incoming call. If no caller information exists, then the mobile computing device performs, as part of the retrieval process, a network retrieval to access the caller information from the network authority.

A platform as described, which includes the operating system level functionality which enables the network retrieval, can be optimized or otherwise configured to minimize latency and network retrieval time, in order to ensure a caller or sender contact information is timely displayed (e.g., before the time the user is likely to notice or respond to the incoming call). In variations, a computing device can perform the network retrieval asynchronously so as to populate, for example, (i) a call log with caller contact information from the network authority after a call has been answered or passed through to voicemail, or (ii) an entry of a messaging folder, representing a messaging item transmitted by a sender, with sender contact information provided from the network authority.

According to some examples, a computing device includes an operating system that includes functionality for performing a retrieval process to a caller or sender contact information service operated by a network authority. The caller or sender information service may provide trusted (e.g., valid and authentic) caller or sender contact information. In some examples, the computing device operates to retrieve caller contact information for an incoming call from the caller information service.

In some examples, the inclusion of operating system level functionality can specialize a computing device on which a retrieval for caller/sender contact information is performed automatically in connection with an incoming call or newly received message. Among other benefits, such operating system level functionality can be implemented without an ability of third-parties to deviate from the implemented functionality. While some variations provide for a user to specify settings as to the performance of functionality as described (e.g., whether caller information retrieval is "on" or "off"), examples may be implemented to preclude other parties (e.g., carrier, caller, user) from altering the functionality implemented at the operating system level. For example, when the network retrieval is performed in connection with an incoming call, examples provide that the computing device uses a network connection to access the network authority, and no other third-party source, in order to determine the caller information for the incoming call. Likewise, in some examples, caller information originating from a source other than network authority, or in some variations, the local resources of the user, may be suppressed or otherwise precluded from being rendered as being inauthentic.

One or more aspects described herein provide that methods, techniques and actions performed by a computing device are performed programmatically, or as a computer-implemented method. Programmatically means through the use of code, or computer-executable instructions. A programmatically performed step may or may not be automatic.

One or more aspects described herein may be implemented using programmatic modules or components. A programmatic module or component may include a program, a subroutine, a portion of a program, a software component, or a hardware component capable of performing one or more stated tasks or functions. In addition, a module or component can exist on a hardware component independently of other modules or components. Alternatively, a module or component can be a shared element or process of other modules, programs or machines.

Furthermore, one or more aspects described herein may be implemented through the use of instructions that are executable by one or more processors. These instructions may be carried on a computer-readable medium. Machines shown or described with figures below provide examples of processing resources and computer-readable mediums on which instructions for implementing some aspects can be carried and/or executed. In particular, the numerous machines shown in some examples include processor(s) and various forms of memory for holding data and instructions. Examples of computer-readable mediums include permanent memory storage devices, such as hard drives on personal computers or servers. Other examples of computer storage mediums include portable storage units, such as CD or DVD units, flash or solid state memory (such as carried on many cell phones and consumer electronic devices) and magnetic memory. Computers, terminals, network enabled devices (e.g., mobile devices such as cell phones) are all examples of machines and devices that utilize processors, memory, and instructions stored on computer-readable mediums. Additionally, aspects may be implemented in the form of computer programs.

System Overview

FIG. **1** illustrates a computing device and system for rendering caller or sender contact information (collectively or alternatively "contact information") from a trusted and authoritative contact information service, according to one or more examples. According to an example of FIG. **1**, a contact information system **10** includes a computing device **100** and an authoritative contact information system **150**. The computing device **100** can correspond to a mobile computing device which includes wireless broadband and cellular connectivity for enabling voice and data network functionality. According to some examples, the computing device **100** can correspond to any device which can receive incoming phone calls and execute functionality to retrieve caller contact information from an independent network authority. According to other examples, the computing device **100** can correspond to any device which can receive messages, such as SMS messages, and execute functionality to retrieve sender contact information from an independent network authority. Still further, in some examples, the computing device **100** can retrieve both caller and sender contact information from the independent network authority, in connection with phone and messaging services provided on that computing device. By way of example, the computing device **100** can include a mobile computing device having capabilities for receiving and initiating phone calls over a cellular connection (e.g., voice channel), PSTN connection and/or IP connection. In some variations, the computing device **100** can include a mobile computing device having capabilities for receiving messages (e.g., SMS messages) over a cellular or IP network channel. Such mobile computing devices may also perform other types of operations, such as data network operations (e.g., Internet browsing) using a Wireless Fidelity (e.g., 802.11(a), 802.11(b), 802.11(g), 802.11(n), Wi-Fi Direct, etc.) or cellular connection. In variations, the computing device **100** can be implemented under alternative computing platforms, such as either a personal computer (e.g., desktop or laptop computer), a dedicated telephony device with data network connectivity, or a cable box or service with Voice-Over Internet Protocol ("VOIP") telephony.

The contact information system **150** can be implemented through an authoritative provider in order to provide a secure and trusted database service for computing devices on which telephony and/or messaging operations are performed. When implemented in connection with telephony services, the contact information system **150** provides independent and trusted caller contact information to the computing device **10** when the computing device **10** receives incoming calls. When implemented in connection with messaging services, the contact information system **150** provides independent and trusted sender contact information to the computing device **10** when the computing device **10** receives a new message. According to one aspect, the contact information system **150** can represent a platform and carrier independent service that is implemented under rules which subjugate the providers of hardware resources (e.g., device manufacturer), software resources (e.g., operating software manufacturer), and network services (e.g., cellular provider) with respect to specific aspects of telephony services (e.g., voice connections made through the PSTN), and specifically with respect to behavior of the phone application when an incoming phone call is received. As described in greater detail, the contact information system **150** can provide a secure network communication source for providing caller or sender contact information over a data network connection. In this way, a receiving device is able to display caller contact information for an incoming call from a trusted and authoritative source. As an addition or variation, the receiving device is able to display sender contact information for a new message from the trusted and authoritative source. In an example of FIG. **1**, the computing device **100** can form a secure network connection with the contact information system **150** over the Internet, using a network port as described below, in order to retrieve and display the contact information in context of an incoming call or new message.

In an example of FIG. **1**, the computing device **100** includes a cellular port **102**, a wireless network port **104**, a display **106**, a speaker **119**, and a processor **110**. Additionally, the computing device **100** can include one or more kinds of memory resources, such as provided by operating system memory **116** (e.g., Read Only Memory or "ROM")) and application memory **118** (e.g., Random Access Memory or "RAM"). The cellular port **102** can enable cellular voice communications, while the wireless network port **104** enables, for example, high-bandwidth wireless (or network) communication suitable for Internet protocol ("IP") data communication applications and resources (e.g., an 802.11 protocol, or "Wi-Fi"). Still further, the wireless network port **104** can also be used for voice communications using a wireless medium such as Wi-Fi. For example, some service providers can enable voice or data communications through non-cellular wireless communication ports (e.g., cellular service providers can enable voice calls to be received or made through a Wi-Fi connection). In some implementations, the selection of the particular communication port can be made dependent on the factors such as the device location, the device's connection quality or strength through the respective communication ports, user preference, device software or hardware resources, or other considerations. In other variations, the cellular port **102** can enable both voice and data communications for purpose of implementing an example of system **10**. Additionally, in some variations, the computing device **100** can utilize a telephony port, such as a wireline interface for the communication network **11**, rather than, for example, cellular port **102** to receive and transmit calls. Thus, in implementation, the computing device **100** can have more or fewer communication ports, with each communication being enabled for voice, data or voice and data. Moreover, one or more additional communication ports can be included with the computing device **100** for enabling communications using alternative wireless or wireline communication mediums.

In an example of FIG. **1**, the computing device **100** may execute instructions **117** for operating a phone application **112**, with a network retrieval component **114** being integrated or functionally linked to the phone application **112**. As an addition or alternative, the computing device **100** executes the instructions **117** for operating a messaging application (SMS application **113**), with the network retrieval component **114** being integrated or functionally linked to the messaging application. In either implementation, variations implement the network retrieval component **114** as an operating system level component for the phone application **112** and/or the SMS application **113**.

In some examples, the operating system memory **116** may maintain device credential **118**, in the form of an encrypted datum that identifies and/or validates the computing device **100** and/or the user of the computing device **100**. In some implementations, the network retrieval component **114** can be an integrated functional element or aspect of the phone application **112** or the SMS/MMS application **113**. In this regard, the phone application **112**, SMS/MMS application **113**, and/or the network retrieval component **114** are implemented as operating level functionality on the computing device **100**. In variations, the application memory

In operation, the computing device **100** receives an incoming communication from a contact device **15**. The incoming communication may be an incoming call connect **101**A or a new message **101**B. The incoming communication **101** may be received on the computing device **100** via, for example, the communication network **11**. In response to receiving the incoming communication **101**, the computing device **100** determines a communication identifier for the incoming communication **101** (e.g., phone number), and then uses the communication identifier to perform a separate network retrieval from the independent network authority **150** to obtain contact information **105** for the contact (e.g., caller or sender) of the incoming communication **101**. In some examples, the incoming communication **101** is a call connect **101**A, and the contact information **105** is obtained and displayed to augment or replace, for example, conventional caller identifier information. In variations, the incoming communication **101** is a new message **101**B, and the contact information is obtained and displayed as part of, for example, the message header or identifier when the message is listed in a folder (e.g., inbox) or opened for viewing. As described in greater detail, the contact information **105** may include rich content (e.g., logos and images, text, textual information about the contact, etc.) that is created and/or configured by the contact. In this way, the network authority **150** enables entities who are owners or holders of communication identifiers to specify contact information **105** that is displayed on their behalf when those entities perform a corresponding communication activity (e.g., make a phone call, send a message). Furthermore, the rendering of the contact information **105** on the computing device **100** provides confirmation to the receiver regarding the identity of the contact who is responsible for the incoming communication **101**.

In one implementation, the cellular port **102** and/or processor **110** can include or operate with caller logic **108** and/or messaging logic **109**. The caller logic **108** may be implemented to detect, process and receive the respective incoming call **101**A, and further to determine the communication identifier **103** of the caller or sender (e.g., phone number). The messaging logic **109** may be implemented to similarly receive and process incoming messages (e.g., SMS messages). While an example of FIG. **1** depicts the incoming communication **101** as being received on the cellular port **102**, in variations, the incoming communication can be received on an alternative communication port, such as the wireless network port **104** (e.g., Wi-Fi port or wireline port). Thus, as an addition or variation, the caller logic **108** can be provided on the wireless network port **104** (or other communication port) to receive the incoming call **101**A, and to determine information from the incoming call, such as caller communication identifier **103**. Additionally, some variations provide for the messaging logic **109** that resides on cellular port **102** or wireless network port **104** (or other communication port) to receive a new message **101**B (e.g., SMS), and to determine information from the new message, such as sender communication identifier **103**.

In response to receiving the incoming communication **101**, the processor **110** sends an outgoing retrieval communication **107** to contact information system **150**. The outgoing retrieval communication **107** may include the communication identifier **103** of the incoming communication **101**, as well as credential information **119** associated with the computing device **100**. The credential information **119** can be based or derived from the credential **118** that is stored on the computing device **100**. In some examples, the credential **118** can include a token or key which is dedicated for use with the contact information system **150**. In response to transmitting the outgoing retrieval communication **107**, the computing device **100** may receive the contact information **105** from the contact information system **150**. The contact information is provided to the computing device **100** in a form that is renderable on the platform of the computing device **100**, and for an appropriate context (e.g., call screen or with messaging item). In the case of an incoming call, the contact information **105** can be rendered while the incoming call **101**A is being received, but before the incoming call is connected (e.g., before the user answers the call).

In an implementation in which the contact information **105** is retrieved for the new message **101**B, the contact information **105** may be retrieved and displayed simultaneously with, for example, a message notification generated on the computing device **105**. In such examples, the messaging application **113** of the computing device **100** may operate to suppress the message notification until the contact information **105** is retrieved, or until a retrieval operation is performed. In some examples, a background process is triggered by the messaging logic **109** to manage retrieval and inclusion of contact information with the header or other portion of the newly received message. In variations, the messaging application **113** can trigger the network retrieval asynchronously, or independently of a corresponding message notification, and then render a message header of the new message with the contact information **105** when the messaging application is operated to display new messages.

In an example of FIG. **1**, the outgoing retrieval communication **107** is communicated to contact information system **150** using the wireless network port **104**. In some operational environments, the configuration provides a benefit of the outgoing retrieval communication **107** being transmitted using a high-bandwidth communication medium, so as to minimize latency in the receipt of the contact information **105**. In some implementations (e.g., when Wi-Fi is not available), the cellular port **102** can also be used to communicate the retrieval communication **107** and to receive the contact information **105**. Still further, alternative configurations can be implemented such that the cellular port **102** is used to transmit the outgoing retrieval communication **107** when the incoming communication **101** is received on either the cellular port **102** or wireless network port **104**.

According to some examples, the contact information system **150** can include functionality such as shown by device interface **152** and contact information database **154**. The device interface **152** can process requests corresponding to network retrieval operations performed on individual computing devices. The contact information database **154** can correspond to, for example, a database structure which maps communication identifiers (e.g., phone numbers, account messaging identifiers) to contact information. As described with some examples, the contact information database **154** can obtain caller or sender contact information from a variety of sources. The device interface **152** can receive the retrieval communication **107** and identify the communication identifier **103** as part of a query **155**. The caller query **155** can be handled by a query processing component **158**, which references the communication identifier **103** with corresponding caller information **105** that is provided in the contact information database **154**.

In implementations which display caller contact information, computing device **100** can receive the contact information **105** from the contact information system **150** when the incoming call **101**A is received. The contact information **105** can be rendered while, for example, an incoming call **101**A is pending on the computing device **100**. In some implementations, caller contact information **105** is rendered on the computing device **100** before the call is shown to the user, or alternatively, before the call is answered. In the latter implementation example, the incoming call **101**A can be displayed briefly without caller information, then displayed with caller information when received. In such examples, the incoming call **101**A can be received and held as pending through the phone application **112** while the network retrieval component **114** retrieves the caller contact information **105**. In some variations, the phone application **112** can suppress user-interface features, such as those used to display caller information **105**, until the caller information is received from the contact information system **150**. The processor **110** receives the caller information **105** via the wireless network port **104**, and then renders caller content **115** based on the retrieved caller contact information **105**. The caller content **115** can be based on or derived from the caller contact information **105**. The caller content **115** can be rendered as text or media using the display component **106**. In variations, the caller content **115** can be generated in whole or in part as audio output.

In some variations, the phone application **112** includes logic to control when the network retrieval component **114** performs the retrieval operations. In one implementation, the processor **110** performs a retrieval process in which an initial determination is made as to whether the incoming communication **101** is associated with a contact record on the computing device **100**. In one implementation, the phone application **112** or messaging application **113** can initiate a local retrieval **121** query from the application memory resource **118** when the incoming call **101** is received. In one implementation, the local retrieval query **121** can check locally stored application data, such as call logs or contact records, for contact information **123** that matches the communication identifier (e.g., phone number). In a variation, a local retrieval query **121** can be communicated to a connected resource of the computing device, such as another connected device. If, for example, the local retrieval query **121** fails to generate a result, the phone application **112** (or other operating system level logic) can trigger the network retrieval component **114** to query the contact information system **150**.

In some variations, the network retrieval component **114** initiates transmission of the retrieval communication **107** concurrently with performance of the local retrieval **121**. Thus, the computing device **100** may receive the contact information **105** with the contact information **123** from a locally stored contact. In such implementations, the phone application **112** can implement a prioritization or rule-based process to suppress information from one source (e.g., caller information **105**) over information from another source, or to display both sets of information (e.g., caller information and contact information **123**) together. Thus, the contact content **115** can be based on both the contact information **105** and the contact information **123**. Thus, in some variations, the outgoing retrieval communication **107** can be transmitted regardless of whether a contact record exists with the resources of the computing device **100**.

In such an example, the rendering of the contact information **105** as contact content **115** can be determined or based at least in part on whether the computing device **100** has contact information associated with the communication identifier **103**.

Caller Information Services

In one example, the contact information system **150** can include, or operate in connection with, an aggregation

component **162**. The aggregation component **162** can represent one or more aggregation processes which access various databases and resources for contact information in order to aggregate caller information (e.g., phone number and caller identifier). In this way, the aggregated caller information can originate from sources, such as governmental registries and/or commercial corporate databases (e.g., such as provided by DUN & BRADSTREET or LINKEDIN). Accordingly, in some examples, the aggregation component **162** can be implemented using source-specific connectors, in combination with a set of database retrieval queries which retrieve contact information. The aggregation component **162** can also determine if caller information already exists for when caller information is retrieved on an ongoing basis for phone numbers and entities. If the aggregation component **162** determines that contact information for a phone number exists, the aggregation component **162** can determine to update or augment the existing caller information using predetermined logic. For example, the predetermined logic can prioritize or sort caller information based on associated attributes or parameters of the entity associated with the corresponding phone number.

As an addition or alternative, the contact information system **150** can include a contact party interface **156** which enables a calling or messaging party user (e.g., representative or agent of a calling party) to provide various inputs **151**, including content input to specify contact content **155**. For example, the contact party interface **156** can correspond to a manual or programmatic interface which enables a contact entity (e.g., corporate entities, organizations, or person) to create, configure, modify or augment information about the entity for display on a receiving device at the time the contacting entity initiates a phone call or sends a message. The contact party interface **156** can enable a calling party to create new information elements for their own contact information, as well as specify design elements of the caller information (e.g., appearance, logo, formatting, etc.). In some examples, the information provided through the contact party interface **156** can be validated by manual or programmatic resources of the authoritative entity. Among other types of information, the contact party interface **156** can enable a contacting party to specify what information (e.g., type, kind, etc.) is displayed to a receiving party when the contacting party initiates a phone call, as well as the appearance such information is to have on the receiving device. As another example, the contact party interface **156** can enable the contacting party to specify content elements, such as logo images, for display in connection with a transmitted message (e.g., SMS message). The specified contact element can be included with, for example, a message header of an outgoing message to the end user device, so that the contact element is visible as part of a user's message inbox or folder.

In other examples, the calling party interface **156** can receive preferential settings **157** which can define a condition by which one or more contact-specified content elements are to be displayed in connection with an initiated call or outgoing message of that contact. For example, a contact may correspond to an individual, who can specify a preferential setting **157** that corresponds to a time setting (e.g., time of day and/or a day of the week). In some implementations, the preferential setting **157** may specify durations of time (e.g., weekdays 9:00 am-6:00 pm) during which select contact-specified content is to be used for calls initiated by the contact. Among other benefits, such implementations enable individuals to have dual-purpose mobile devices, such as for work/business and personal. When the user makes a call within a duration specified by the user's preferential setting **157**, contact information system **150** may retrieve contact content for the caller that is for the business that employs the caller, while a call outside of the specified setting may result in contact information system **150** retrieving content that identifies the individual making the call.

Still further, in some examples, contact information system **150** may include analytic logic **170** to monitor usage of communication identifiers by callers or senders. For example, if an extraordinary number of retrieval requests are specified for a particular phone number by a population of device users within a given time frame (e.g., an hour or a day), the analytic logic **170** may detect the occurrence and proactively flag or indicate the communication identifier as being associated with a solicitation service. In subsequent retrieval requests from the population of users, contact information system **150** returns contact information which includes, or otherwise identifiers the caller or sender as a likely solicitor. In this way, contact information system **150** can proactively identify likely solicitors to computing devices **100** of a population in connection with unwanted phone calls or messages. The users of the computing devices may further employ filters to, for example, preclude receipt or handling of incoming communications from the contacts who are deemed to be solicitors.

Device Functionality for Use with Caller Information Service

In some examples, the processor **110** executes the instructions **117** to generate a set of user interface features when the caller information content **115** is rendered. The user interface features can generate prompts for user input when the caller information content **115** is rendered. When user input is received in connection with a given user interface feature, the processor **110** may be triggered to perform a set of operations which utilize the caller information **105**. By way of example, the set of operations can include (i) storing information provided from the caller information **105** as part of a local contact record on the computing device **100**, using the application memory resources **118**, and/or (ii) generating a network communication that reports information about the incoming call **101** to the authoritative entity or other network service.

According to one implementation, the processor **110** can store the caller contact information **105** as a contact record **127** using, for example, the application memory resources **118**. Alternatively, the caller information **105** can be used to augment an existing contact record **127**. For example, the caller contact information **105** can include information which may not exist in the contact record of the user of the computing device **100**.

Still further, a user interface feature can be generated through the phone application **112** to generate a network communication **131** which reports information about the incoming call **101**A. The network communication **131** can, for example, be signaled in response to user input when the incoming call **101**A is unsolicited or not authentic. For example, when the caller information content **115** is rendered on the display component **106** of the computing device **100**, a user interface feature (e.g., see network notification feature **336**, FIG. **3**C) can be displayed to enable the user to mark a complaint with the incoming call. For example, the call may be an unwanted solicitation, or from a caller who is masking their true origin. The user can interact with a network notification feature **336** (see FIG. **3**A through FIG. **3**C) to signal their complaint. The processor **110** can then generate the network communication **131** to a corresponding network location, such as provided by the contact information system **150**. In some variations, the user may be prompted to enter information regarding the nature of the communication, such as the basis of the user's complaint.

In this way, the network communication **131** can be generated by the user as a mechanism to report a complaint. In one example, the network communication **131** can be communicated via the wireless network port **104** to the contact information system **150**. The network communication **131** can be recorded in association with the caller information **105** for the incoming call **101**.

In some examples, the contact information system **150** can record instances when network communication **131** are generated for a particular phone number, or alternatively for a particular entity which may manage multiple phone numbers. The contact information system **150** can tabulate instances when the network communications **131** are generated from different devices. When, for example, the number of communications **131** exceed a threshold, the associated phone number which generated the communications (e.g., complaints) from the various devices can be flagged as being problematic (e.g., unsolicited caller).

Caller Interface Examples

FIG. **3**A through FIG. **3**C illustrate variations of a caller interface **300**, according to one or more examples. In examples shown, the caller interface **300** is shown to display different types of caller content **115** when a corresponding incoming call is received. The caller interface **300** can be triggered for display on the display component **106** when an incoming call **101**A is initially received.

With reference to FIG. **1** and FIG. **3**A through FIG. **3**C, the caller interface **300** can be used to display caller contact content **115**, which can include, for example, (i) alternative phone numbers **302** which a receiving party can use to contact the calling party; (ii) messaging identifiers **304** for use by a receiving party to message the calling party, (iii) a website **306** or network location where additional information about the calling party is made available, (iv) a logo **308**, including an image or other media content for rendering on the computing device of the receiving party. In some variations, the caller interface **300** can include a set of user interface features **312**, **314** which are actionable with user input in order to cause the processor **110** to perform a predetermined set of actions using the caller contact information **105**.

As described with other examples, the caller interface **300** can also include actionable user interface features for enabling the computing device **100** to perform an action using or based on the displayed caller information **105**. In examples of FIG. **3**A through FIG. **3**C, a contact feature **332** can be provided which the user can interact with in order to store the caller contact information **105** with or as part of a new contact record. In this way, the user can, for example, store alternative phone numbers, message identifiers, and websites of a calling party. Another example of an actionable feature **334** is a local caller block function, which the user can use to block future incoming calls from the same phone. The actionable feature **334** may also be used in examples in which contact information system **150** proactively indicates an incoming call is a solicitation.

In another variation, the caller interface **300** can include the network notification feature **336** which the user can interact with in order to generate, for example, the network communication **131**. As described with other examples, the network notification feature **336** can provide a mechanisms by which the caller can signal a complaint about the incoming caller. When the user interacts with the notification feature **336**, one example provides that the network communication **131** is sent to the contact information system **150** (e.g., via the cellular port **102** or the wireless network port **104**) that identifies the communication identifier **103**, as well as a value or data element provided through the notification feature **336** which indicates the user is complaining about the caller. The contact information system **150** can record information about the event, such as the occurrence of the event, the time the event occurred, and/or the user or computing device which made the complaint.

As described with other examples, the contact information system **150** can include logic, such as rule based logic, which tallies or aggregates complaints for individual callers, such as by phone number or caller identifier of the caller. The contact information system **150** can implement rules, for example, which provide that if a particular caller (e.g., organization responsible for a particular number) receives too many complaints in total, or if a caller receives too many complaints in a given duration of time (e.g., 1 month), remedial action can be taken such as the caller being warned or fined.

In variations, the actionable feature **334** can serve dual roles in which the user can block the caller from calling the user's computing device, as well as providing a mechanism in which the user's interaction with the feature results in the network communication **131** being communicated to the contact information system **150**. The contact information system **150** can then implement logic to determine when/if remedial actions are needed against the caller.

Message Interface Examples

FIG. **4** illustrates an example message interface for use with a computing device, according to one or more examples. In an example shown, a message interface **400** is shown to display sender contact information, in the form of content elements **410** which may be specified or selected by the user.

In some examples, the message interface **400** may be implemented for a messaging application which utilize phone numbers as the primary communication identifier. In numerous examples, this is described as an SMS messaging application. In variations, the messaging interface may be provided for proprietary applications, such as iMessage (provided by APPLE INC.). The computing device **100** may receive a new message from, for example, a business, or an individual associated with a business. The computing device **100** may perform the retrieval for sender contact information, as an independent network authority. In some variations, this may be performed when, for example, the messaging application does not recognize the phone number used by the sender.

In some implementations, the retrieved sender contact information **105** may include a logo and/or text content. In variations, the retrieved sender contact information **105** can include an audio jingle, animated picture or other media content item. As with other examples, the contact information **105** may be selected by the sender (or business) who controls or owns the phone number.

In some examples, the computing device **100** includes logic to blend or integrate the retrieved content element with the contents of the message as received on the computing device. For example, logos **410**, **412** may be received from the contact information service **150** independent of the respective incoming message **401**, **403**. The logos **410**, **412** may be assembled or integrated into the respective message **401**, **403** when the message is displayed in list form with other messages (e.g., as part of an inbox). Thus, the sender can use the contact information system **150** to specify logo or other branding content, which is then displayed on the receiving device, without need for the sender to include the logo or branding content at time of transmission. In some variations, the sender contact information **105** (e.g., logo **410**, **412**) may also be displayed with other context, including when the message is rendered individually, and/or as part of a message notification which informs the user that a new message has arrived.

Methodology

FIG. **2**A illustrates an example method for implementing a contact information service on a computing device of the user, according to one or more examples. A method such as described with an example of FIG. **2**A can be implemented using a system such as described with an example of FIG. **1**. Accordingly, reference to elements of FIG. **1** is to illustrate suitable components or elements for performing a step or sub-step being described.

In an example, the computing device **100** receives an incoming communication (e.g., phone call, SMS message) and determines a caller identifier (e.g., phone number) (**210**).

The processor **110** can initiate a retrieval process for determining the caller or sender contact information, using the communication identifier (e.g., phone number) of the incoming communication **101** (**220**). In one implementation, the processor **110** performs a local retrieval operation to determine if contact information exists on the computing device **100** which matches the communication identifier (e.g., phone number) of the incoming communication **101** (**222**). As an addition or alternative, the processor **110** performs a network retrieval operation to retrieve the caller or sender contact information **105** from the contact information system **150** (**224**). The processor **110** can then render the retrieved caller or sender contact information **105** using the display **106** and/or speaker **109** (**230**).

Other Examples

While numerous examples are described in the context of an end user device performing a network retrieval at or near a time when an incoming message is received, variations provide that providers of end user devices may alternatively (or additionally) perform network retrievals of the content information system **150** when end user devices of those providers receive the incoming calls or messages. For example, a carrier (e.g., for cellular or VOIP telephony) may perform the network retrieval from the contact information system **150**, for an incoming call directed to a customer device prior to, or concurrently with the incoming call being forwarded to the customer device for call handling. In some implementations, the provider (e.g., carrier) may perform the operation on behalf of (or in place of) the customer device.

In other variations, providers may couple the use of contact information system **150** with other verification services to reduce a number of instances in which the carrier/provider networks are used to conduct unwanted solicitations and/or fraud. Some providers, for example, utilize verification services to ensure a phone number of a caller is not spoofed, but legitimate. In some examples, such providers may further use the contact information system **150** to determine if the caller is a likely solicitor. For example, in one implementation, the contact information system **150** may be integrated or combined with a verification service that returns, to a provider making a retrieval request, a communication that verifies the phone number being used is not spoofed, and confirmation that the phone number is not associated with an entity that is known to make solicitations or commit fraudulent activity. FIG. **2**B illustrates an example method for implementing a contact information service on a distributed receiving-end computer system. A method such as described with an example of FIG. **2**B may be implemented using functional components such as described with FIG. **1**, implemented in part or whole on alternative computing environments, as described in more detail by examples provided below.

In an example of FIG. **2**B, a receiving end computer system receives an incoming communication, specifying a communication identifier of a contact who initiated the communication (**240**). The incoming communication may correspond to, for example, an incoming phone call or message. In some examples, the incoming communication may correspond to a telephony call, initiated by a caller contact and terminated at the receiving computing system using an IP network (e.g., VOIP call). As an addition or alternative, the incoming communication may correspond to, for example, an incoming message, initiated by a sender contact. In some examples, the incoming communication specifies the phone number of the contact (or of the contact's device).

In one implementation, the receiving-end computer system corresponds to a computing device operated by the end user (e.g., computing device **100**) (**242**). Thus, for example, the receiving-end computer system may be implemented as described with an example of FIG.

In a variation, the receiving-end computer system includes a provider computer system and a user computing device (**244**). Still further, in another variation, the receiving-end computer system includes multiple computing devices operated or controlled by the end user (**246**).

The receiving-end computer system may use the communication identifier of the incoming communication to perform a retrieval process in order to determine the caller or sender contact information (**250**). In some examples, the receiving-end computer system perform the retrieval process using a rendering computing device operated by the user, so that the computing device that retrieves the contact information **105** and then renders corresponding content is the same (**252**).

According to another aspect, the receiving-end computer system performs the retrieval process to obtain contact information **105** from the contact information service **154** using a provider-operated computing system, and the contact information is then forwarded to the end user computing device for rendering (**254**). For example, the receiving-end computer system may include a carrier server component that implements the retrieval process as part of a verification process, then forwards the incoming communication to the computing device (e.g., cellular or wireless telephony device) of the end user. As another example, the receiving-end computer system may be operated by a VOIP provider who performs the retrieval process to obtain the contact information **105** from the contact information system **154**, before or at the time the incoming communication (e.g., phone call) is received. The VOIP provider may then forward the incoming call to a corresponding end user device for handling VOIP calls. In some examples, a first device (e.g., set-top box) receives the incoming communication along with the contact information **105** from the provider component, and then distributes the contact information for rendering on a first device (e.g., television) and a second device (e.g., VOIP phone).

Still further, the receiving-end computer system may include multiple computing devices which are operated by the user, with a first computing device performing the retrieval process to obtain the contact information **105** from the contact information system **154**, and a second device rendering content from the retrieved contact information (**256**). For example, a cable user may operate a set-top box that automatically performs the network retrieval process to obtain the sender or call contact information whenever an incoming communication is received through that device. In the user's computing environment, another computing device (e.g., television) may be used to display the contact information of the caller or sender. Still further, a third device (e.g., dedicated VOIP phone) may be used to receive the communication.

Hardware Diagram

FIG. **5** is a block diagram that illustrates a computer system upon which examples described herein may be implemented. A computer system **500** can be implemented on, for example, a server or combination of servers. For example, the computer system **500** may implement contact information system **150**, as described in an example of FIG. **1**.

In one implementation, the computer system **500** includes one or more processors **510**, memory **520** (e.g., a read-only memory (ROM), a storage device, RAM) and a communication interface **550**. The computer system **500** includes at least one processor **510** for processing information stored in the memory **520**. The memory **520** also may be used for storing temporary variables or other intermediate information during execution of instructions to be executed by the processor **510**. In some examples, the memory **520** stores, for example, the contact database **154**, or retrieved portions of the contact database from which further processing may be performed. The memory may also store contact information system instructions **522** for implementing contact information system **150**, as shown with some examples of FIG. **1**.

The communication interface **550** enables the computer system **500** to communicate with end user devices (e.g., smart phones, cable boxes, personal computers) over one or more networks **680** (e.g., cellular network. PSTN, IP network) through use of the network link (wireless or wired). Using the network link, the computer system **500** can communicate with one or more computing devices, as well as computer systems of providers (e.g., cellular carriers). The processor **510** is configured with software and/or other logic, shown as caller information system instructions, to perform one or more processes, steps and other functions described with caller information service **150** of FIG. **1**.

Some examples described herein are related to the use of the computer system **500** for implementing the techniques described herein. According to one example, those techniques are performed by the computer system **500** in response to the processor **510** executing one or more sequences of one or more instructions contained in the memory **520**. Execution of the sequences of instructions contained in the memory **520** causes the processor **510** to perform the process steps described in connection with contact information system **150**. In alternative implementations, hard-wired circuitry may be used in place of or in combination with software instructions to implement examples described herein. Thus, the examples described are not limited to any specific combination of hardware circuitry and software.

Although illustrative aspects have been described in detail herein with reference to the accompanying drawings, variations to specific examples and details are encompassed by this disclosure. It is intended that the scope of examples described herein be defined by claims and their equivalents. Furthermore, it is contemplated that a particular feature described, either individually or as part of an embodiment, can be combined with other individually described features, or parts of other aspects. Thus, absence of describing combinations should not preclude the inventor(s) from claiming rights to such combinations.

What is claimed is:

1. A method for operating a computing device, the method comprising:

(a) determining a phone number of an incoming communication;

(b) initiating a retrieval process to retrieve information associated with the phone number from a predetermined network location of a network authority, wherein the information is retrieved from a database storing phone numbers associated with a plurality of end-user devices, and wherein an entity authorized with the network authority to use the phone number provides the information to the network authority to associate the information with the phone number; and

(c) rendering the retrieved information and the phone number of the incoming communication using the computing device.

2. The method of claim **1**, wherein (a) includes determining the phone number of an incoming call, Short Message Service (SMS) message or Multimedia Message Service message (MMS).

3. The method of claim **1**, wherein (a) through (c) are performed by at least one of a phone application, voice network service or messaging application.

4. The method of claim **1**, wherein at least one of (a) through (c) is performed by an operating level component of the computing device.

5. The method of claim **1**, wherein (a) through (c) are performed on the computing device in response to an incoming call, and while the incoming call is pending on the computing device before being answered.

6. The method of claim **1**, wherein (c) includes displaying branding content of the entity that is authenticated by the network authority as being associated with the phone number of an incoming call or message.

7. The method of claim **1**, wherein (b) includes making a determination as to whether locally stored information is associated with the phone number, and then performing a network retrieval based on the determination.

8. The method of claim **7**, wherein (b) is performed when the determination is that no locally stored information is associated with the phone number.

9. The method of claim **1**, wherein initiating the retrieval process includes making a secure connection to the predetermined network location.

10. The method of claim **1**, wherein the incoming communication is communicated to the computing device over at least one of a Public Switch Telephone Network ("PSTN"), cellular network, or Internet Protocol network.

11. The method of claim **1**, further comprising:

displaying, in connection with an incoming call or message, one or more features to perform a corresponding one or more alternative actions other than answering the incoming call.

12. The method of claim **1**, further comprising:

displaying a feature to enable a user to provide input about an incoming call or message to the network authority.

13. The method of claim **1**, wherein (c) includes displaying the retrieved information as part of a header or message body of an incoming message.

* * * * *

Exhibit 7

Sterne Kessler
STERNE KESSLER GOLDSTEIN & FOX

MICHAEL D. SPECHT
DIRECTOR
(202) 772-8756
mspecht@skgf.com

August 24, 2020

Roger Desai
Chief Executive Officer
Prove (formerly Payfone)
245 5th Avenue, 20th Floor
New York, NY 10016

Via Federal Express

Dear Mr. Desai,

Neustar has made significant investments in caller-authentication services to provide an industry-leading service to our customers, while ensuring marketplace integrity. These investments include the acquisition of TRUSTID in 2019, which filed its first patent application in this space in early 2009 and built a strong patent portfolio that protects the core technical aspects of its caller-authentication technology. In light of these significant investments, Neustar is fully committed to protecting its intellectual-property rights, including those acquired through its purchase of TRUSTID.

In this regard, Neustar has determined that several of Prove's call authentication services, including but not limited to Prove's Call Center Authentication, Trust Portal, Instant Authentication for Voice and Trust Score service offerings infringe at least the following Neustar patents:

> U.S. Patent No. 9,001,985, entitled *Method of and System for Discovering and Reporting Trustworthiness and Credibility of Calling Party Number Information*, filed Aug. 6, 2012 and issued Apr. 7, 2015, claiming priority to May 19, 2009,
>
> U.S. Patent No. 8,238,532, entitled *Method of and System for Discovering and Reporting Trustworthiness and Credibility of Calling Party Number Information*, filed May 19, 2010 and issued Aug. 7, 2012, claiming priority to May 19, 2009,
>
> U.S. Patent No. 9,871,913, entitled *Systems and Methods to Identify ANI and Caller ID Manipulation for Determining Trustworthiness of Incoming Calling Party and Billing Number Information*, filed Feb. 16, 2016 and issued Jan. 16, 2018, claiming priority to Jan. 20, 2012,
>
> U.S. Patent No. 9,762,728, entitled *Using Calling Party Number for Caller Authentication*, filed Dec. 2, 2016 and issued Sep. 12, 2017,
>
> U.S. Patent No. 10,244,107, entitled *Systems and Methods for Causing Display of a Reputation Indicator Associated with a Called Party*, filed Oct. 27, 2017 and issued Mar. 26, 2019, claiming priority to Oct. 23, 2017, and

U.S. Patent No. 10,033,863, entitled *Determining Porting Histories for Telephone Numbers*, filed Mar. 6, 2017 and issued Jul. 24, 2018.

As you are likely aware, TRUSTID asserted the ’985, ’532 and ’913 patents in a pending lawsuit for patent infringement against Next Caller. Next Caller has failed multiple times before both the United States District Court of Delaware and Patent Trial and Appeal Board (PTAB) to invalidate these patents, further confirming TRUSTID’s innovation and the strength of its patents.

To protect our investments and further support marketplace integrity, we require that Prove not infringe any of Neustar’s patents as highlighted above. We require a response to this letter by Sept 8, 2020 that either confirms that Prove will cease providing the infringing services or explains how its services are not covered by the Neustar patents. In the absence of such a response, we will assume that Prove does not intend to curtail its infringing activities and we will consider any and all actions that may be necessary to protect our intellectual property. Neustar looks forward to amicably resolving this matter.

Sincerely,

/Michael D. Specht/

Michael D. Specht
Director
Sterne, Kessler, Goldstein & Fox

MDS:mlb

Exhibit 8

prove
Formerly Payfone

Easy-to-implement APIs to secure and streamline your customer journey

Request a Meeting

Our award-winning identity verification and authentication APIs make it easy to connect to Payfone's omni-channel customer identity platform

Our identity verification and authentication APIs:

Trust Score

Description

Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes.

Solutions That Leverage This API

- Account Opening
- Existing Customer Authentication
- Fraud Prevention

Fonebook

Description

Enables you to continuously update your customer records against millions of daily change events. Establishes persistent, private IDs for your customers so that their identities can be securely verified during interactions such as mobile and web logins, and call center calls.

Solutions That Leverage This API

- Account Opening
- Existing Customer Authentication
- Fraud Prevention

Identity Pre-Fill

Description

Enables you to securely and privately match information entered by the user with what is on file for them at authoritative sources. Prevents fraudulent account openings.

Solutions That Leverage This API

- Account Opening

Identity Verify

Description

Enables you to securely and privately match information entered by the user with what is on file for them at authoritative sources. Prevents fraudulent account openings.

Solutions That Leverage This API

- Account Opening
- Fraud Prevention

Instant Authentication for Voice

Description

Authenticates inbound call center calls and prevents ANI spoofing.

Solutions That Leverage This API

- Existing Customer Authentication
- Fraud Prevention

Instant Authentication for Mobile

Description

An easier and more secure alternative to SMS OTP that authentic identities passively in real time via a mobile device.

identities passively in real time via a mobile device.

Solutions That Leverage This API

- Account Opening
- Existing Customer Authentication
- Fraud Prevention

Instant Link for Web

Description

An easier and more secure alternative to SMS OTP that authenticates identities in real time by clicking an SMS link.

Solutions That Leverage This API

- Account Opening
- Existing Customer Authentication
- Fraud Prevention

Multi-Factor

Multi-Factor Authentication

Description

Three different options for multi-factor authentication. These capabilities combine something a person HAS, something a person KNOWS and something a person IS to authenticate a high-risk transaction.

3 options for multi-factor authentication

- SMS OTP
- Voice OTP
- Biometrics

Trust Portal

Description

Empower call center and fraud teams to verify customer identities in real time and conduct investigations.

An intuitive portal that enables your customer service teams to verify customer identities and fraud teams to conduct investigations.

Learn More

Let us help you reach your goals with an innovative Trust Platform that enables you to extend faster, frictionless and fraud-free experiences to all of your customers.

Request a Meeting

prove
Formerly Payfone

Home

Trust Platform

Products

Company

Resources

Press and News

Contact Us

Careers Now Hiring

Privacy Policy Exercise Your Rights Do Not Sell My Personal Information

Exhibit 9

Payfone Raises $100 Million Read More ×

TALK TO OUR EXPERTS

Are fraudsters using your call center against you? Learn how Call Center Authentication can help.

Request your consultation

First Name*

Last Name*

Business Email*

Current Call Center Authentication Solution

Phone number (optional)

Request Consultation

Proactive call verification technology to stop fraud before it starts

Call Center Authentication is the world's first full-stack solution that enables enterprises to:

- Preemptively protect their call centers against emerging threats such as IVR (interactive voice response) credential stuffing, ANI spoofing, SIM swap, and account takeover
- Greenlight the majority of callers without subjecting them to frustrating roadblocks such as knowledge-based security questions or one-time passcodes

Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience.

During your consultation, one of our call center specialists will:

- Examine any vulnerabilities your current call center solution might be leaving you open to
- Outline how Call Center Authentication can not only mitigate fraud threats but also help you deliver an enhanced call center experience by cutt handle time by 2-4 minutes
- Walk you through how Call Center Authentication can save significant operating expenses in your call center (an average of $3.60 per call)

Complete the form above and we will be in touch to arrange your consultation.

Not ready for a consultation?

Download a fact sheet instead to see if Call Center Authentication is the right fit for your business.

First Name* Last Name*

Business Email*

Current call center authentication solution (If you don't have one, just write "none")

Phone number (optional)

Download Fact Sheet

www.payfone.com

212 614 6927 info@payfone.com

© 2020 Payfone

Privacy Policy

Exhibit 10

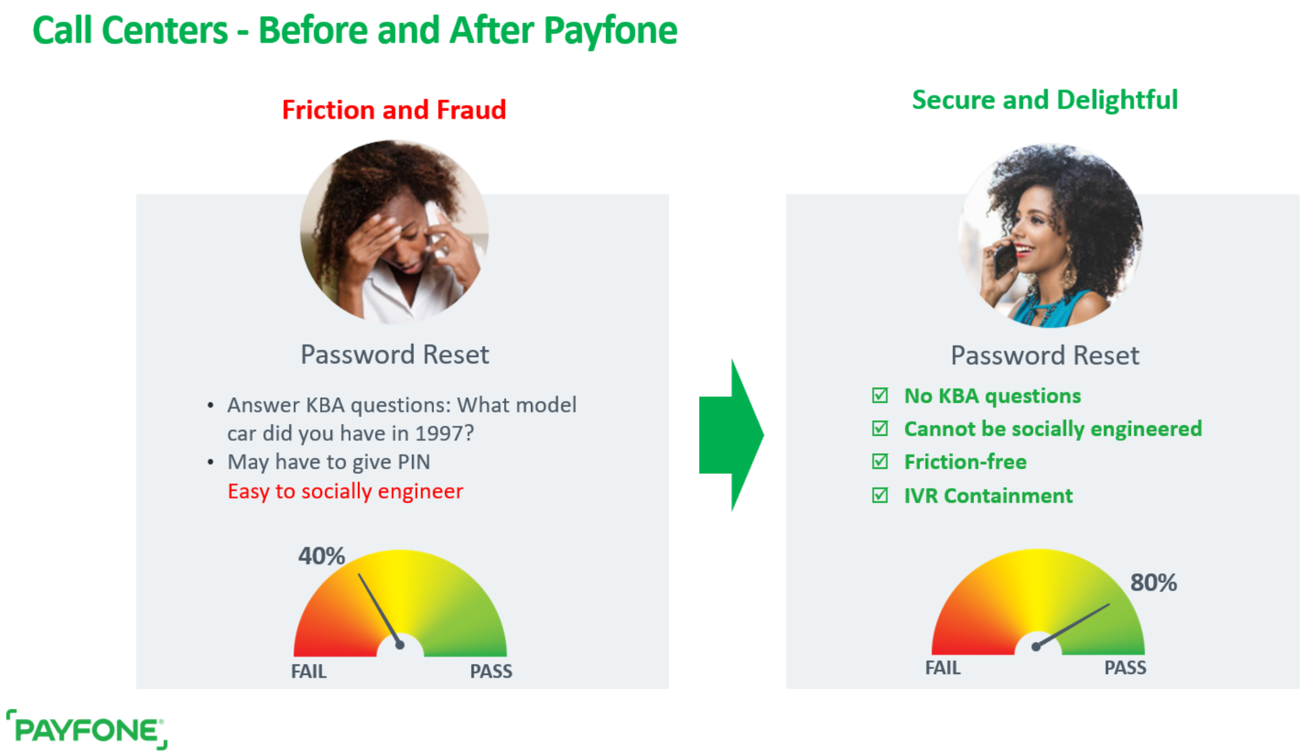
prove
Formerly Payfone

‹ Back to View All

Did You Know?: You Can Assess Your Call Center Authentication Solution with This Handy Checklist

September 18, 2019

Share This Article:



Call Centers - Before and After Payfone

Friction and Fraud

Password Reset

- Answer KBA questions: What model car did you have in 1997?
- May have to give PIN

Easy to socially engineer

Secure and Delightful

Password Reset

☑ No KBA questions
☑ Cannot be socially engineered
☑ Friction-free
☑ IVR Containment

The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.*

The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention.

Curious to see what other features make Payfone's Call Center solution so comprehensive and to see how your current solution stacks up? Down' our Call Center Authentication Checklist below for the most critical differentiators to look for in a solution.

*Source: PYMNTS

Get the Call Center Authentication Checklist

First name*

Last name*

Company name*

Business Email*

Job title

Download the Checklist

Share This Article:

Tags: call center authentication customer experience did you know Digital Identity

prove
Formerly Payfone

Home

Trust Platform

Products

Company

Resources

Press and News

Contact Us

Careers Now Hiring

Privacy Policy Exercise Your Rights Do Not Sell My Personal Information

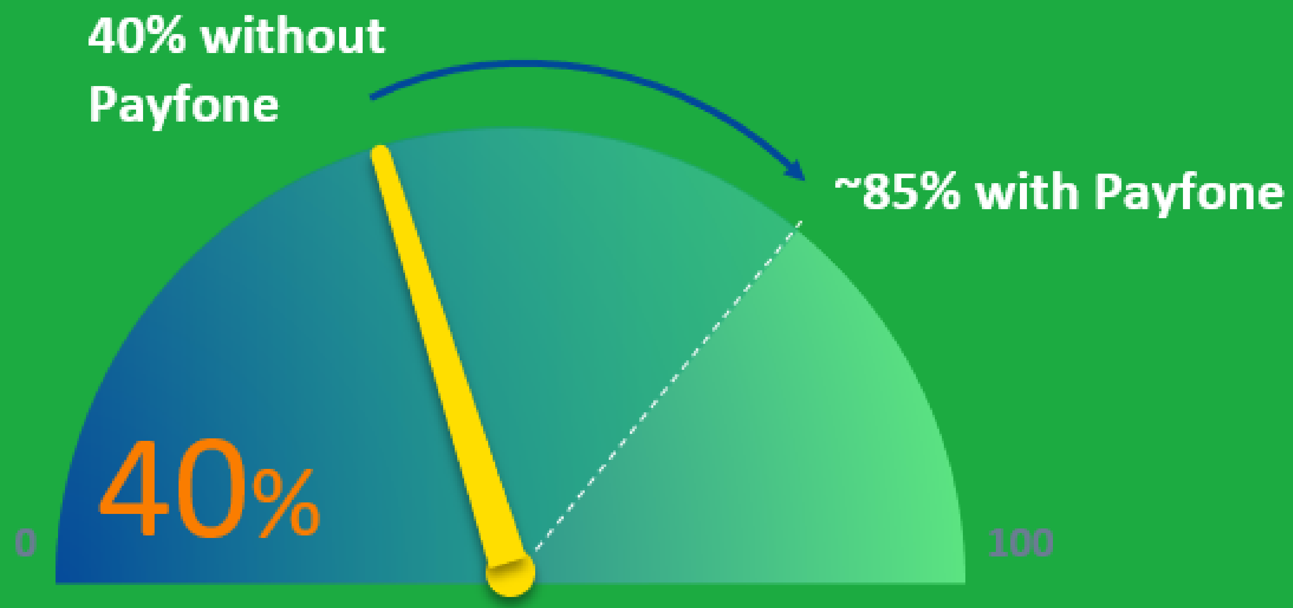
Exhibit 11

PAYFONE®

Transform Your Business with Identity Verification

Safely approve and pass more transactions by instantly identifying customers over mobile or desktop and in call centers. Payfone's Trust Platform and Trust Score™ let you deliver frictionless CX and thwart fraud.

Contact Us To Set Up A Meeting



Close the Trust Gap and pass more customer transactions with Payfone

Fast

Replace slow and insecure identity verification processes such as passwords, security questions and SMS one-time passcodes to give your customers access to your products and services in milliseconds, not minutes.

Frictionless

Unlike traditional ID-proofing methods, Payfone's modernized approach to identity authentication requires no action on the part of the customer, removing unnecessary friction from signups, logins, call center calls and other interactions. Additionally, no app download is needed.

Fraud-Free

Passwords, knowledge-based authentication processes and SMS one-time passcodes are easy to break. Payfone's solutions are fortified against hacking, social engineering, SMS interception and ANI-spoofing.

For Mobile

Activate our Trust Platform for your mobile apps and mobile web to authenticate your customers instantly when they log in, sign up, or interact.

For Call Center

Payfone's Call Center solution enables you to greet your customer with 'Hello' instead of 'Who are you?' and save OPEX by avoiding the need for interactions with customer service representatives.

For Web (Desktop)

Our mobile authentication technology can also be leveraged for desktop web to frictionlessly verify customer identities when they visit your websites or online portals.

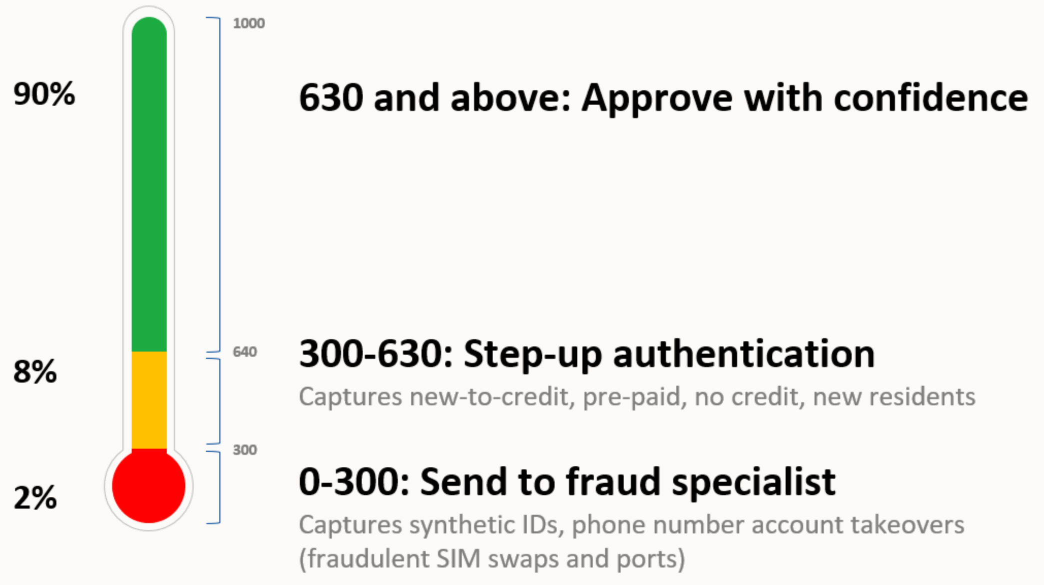
Trust Platform

Payfone’s award-winning **Trust Platform** replaces cumbersome and hackable identity verification processes such as knowledge-based security questions, one-time text passcodes, and passwords with instant, invisible, and privacy-centric (**zero-knowledge**) digital authentication protocols.

Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the ‘**Trust Gap**’ between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions.

Trust Score™

The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question “Should I trust this interaction?”



630 and above: Approve with confidence

300-630: Step-up authentication

Captures new-to-credit, pre-paid, no credit, new residents

0-300: Send to fraud specialist

Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports)

> *"Payfone's solutions will significantly simplify the enrollment processes for millions of **Zelle** P2P users, while adding another layer of non-intrusive protection behind-the-scenes for **Zelle** Payfone brings together data from across the mobile ecosystem – networks, devices, users – to help us assess enrollment and transaction risk almost instantly. This helps us balance the requirements for speed and security in the faster payments space."*

ERIC WOODWARD

Early Warning/Zelle

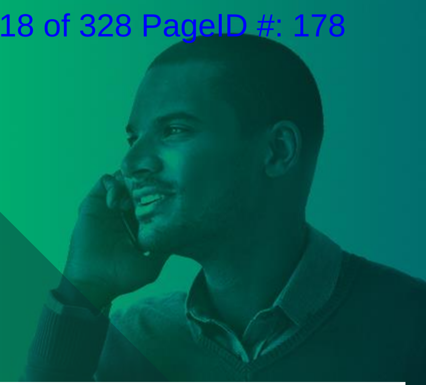
Gain the competitive edge with Digital Trust

Learn how you can enable faster, frictionless and fraud-free experiences for all of your customers

Contact Us To Set Up A Meeting

Exhibit 12

Call Center Authentication Solution Checklist



Curious to see how your call center authentication solution stacks up? Refer to the checklist below for the most critical differentiators to look for in a solution.

		Payfone
□	Does the solution detect and prevent ANI-spoofing?	Yes
□	Does the solution stop fraudulent pin code changes?	Yes
□	Does the solution detect SIM swaps, burner phones, fraudulent ports and account takeovers?	Yes
□	Does the solution eliminate frustrating KBA questions?	Yes
□	Does the solution help contain calls in your IVR?	Yes
□	Does the solution cut handling time and save you OPEX?	Yes
□	Can the solution be applied instantly?	Yes
□	Does the solution provide a **definitive (as opposed to probabilistic or presumed)** answer as to whether the person on the other end of a call is a legitimate caller?	Yes
□	Does the solution deliver the ability to eliminate false positives?	Yes
□	Is the solution impervious to 1st caller fraud?*	Yes
□	Does the solution include direct carrier integration?	Yes
□	Does the solution include sophisticated SIP invite analysis?	Yes
□	Does the solution meet NIST AAL3 (highest level of assurance)?	Yes

Interested in learning more? Visit payfone.com/contact to request more information.

*1st Caller Fraud – the inability to authenticate during the initial call is a vulnerability since the fraudster may be calling the 1st time, and therefore the fraudster's voice and device being mapped.

PAYFONE®

Exhibit 13

Call Centers

Calling a mortgage provider should be as easy as calling a friend. No questions asked

Get Started

WELCOME YOUR CUSTOMERS WITH 'HELLO'

NOT 'WHO ARE YOU?'

Lucas is a partner at a global law firm and has just moved from San Francisco to New York City. Although he stayed with Verizon, Lucas changed his mobile phone number to a local New York number. Lucas calls his mortgage provider, General Mortgage, to update them with his new address. He chooses Saturday morning to do this because he assumed it would be a cumbersome process. Lucas is in for a pleasant surprise; General Mortgage uses Payfone.

LET'S SEE LUCAS'S EXPERIENCE IN ACTION

1 The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone

A week later, Lucas calls General Mortgage's 800 customer service number to update his address

2

3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now

4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions

5 Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?"

6 Lucas couldn't be happier. He has completed the task and is back to his day after only a few minutes

GET MORE INFO

https://www.payfone.com/experiences/call-centers/ Go SEP OCT NOV 03 2017 2018 2019

1 capture
3 Oct 2018

About this capture

OW?

- With Configurable Enrollment Rules and Trust Score, Payfone can now authenticate every login and every digital engagement for every end-user, creating a VIP lane for the legitimate, while delineating known and suspected fraud as well as the unknown for further inspection with step-up authentication processes
- Every second a caller spends with a customer service representative costs the business 1 cent. To verify caller identity through KBA questions takes on average two minutes, resulting in a mean operating expense of $1.20 per call
- Should General Mortgage not recognize Lucas's new office landline, Lucas is sent to a call center team dedicated to unidentifiable callers. General Mortgage sends Lucas an SMS with an Instant Link to his mobile phone. Lucas clicks on the link and now Lucas's New York office landline is added to General Mortgage's Fonebook
- Additionally, using the Payfone Trust Score as guidance, General Mortgage offers Lucas relevant products and services at the end of his call

Get Started

Creating an account is a snap. Get access to:

- APIs
- Product Manager Resources
- Developer Resources
- Info-Sec Resources
- Implementation Guides
- Call Flows
- Data Coverage Stats
- Configurable Enrollment Rules

GET STARTED

Company
Press
Investors
Careers
Contact
Privacy Policy

Technology
Platform
Markets

Products
Instant Authentication for Mobile
Instant Authentication for Voice
Instant Link for Web
Payfone Fonebook
Trust Score
Identity Pre-Fill

Exhibit 14

Trust Score

BE CONFIDENT THAT IT'S REALLY YOUR CUSTOMER

Payfone's Trust Score is the most complete real-time snapshot of identity confidence on the market. Used by Fortune 100 clients ranging from top banks to leading retailers and health insurance companies, The Trust Score analyzes digital signals from a wide array of trusted sources to give you assurance that it's really your customer on the other end of a digital transaction.

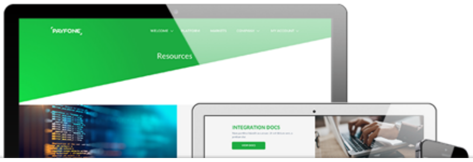
- Omni-channel: Functions across mobile app, mobile web, voice (call center), PCs and tablets to authenticate account openings, logins, text and chat sessions, and inbound and outbound call center calls
- Decentralized: Multiple, differentiated sources to inform and verify identity
- Works through consumers' mobile phones so there is no app needed and nothing to download
- No consumer data is stored
- Stronger identity confidence allows enterprises to extend more services and conveniences to consumers immediately without tenuring
- Thwarts account takeover and impersonation attacks; Impervious to social engineering

LEARN MORE

Ready To Learn More?

Create an account to get access to:

- APIs
- Product Manager Resources
- Developer Resources
- Info-Sec Resources
- Implementation Guides
- Call Flows
- Data Coverage Stats
- Configurable Enrollment Rules



GET STARTED

https://www.payfone.com/products/trust-score/ Go APR OCT APR
3 captures 23
22 Apr 2018 - 15 Apr 2019 2017 2018 2019
About this capture

COMPANY
Press
Investors
Careers
Contact
Privacy Policy

TECHNOLOGY
Platform
Markets

PRODUCTS
Instant Authentication for Mobile
Instant Authentication for Voice
Instant Link for Web
Payfone Fonebook
Trust Score
Identity Pre-Fill

Exhibit 15

Prove (formerly Payfone) announced today that it has seen a 300% YoY increase in new business wins and now serves nine of the top ten financial institutions in the United States.

READ MORE

The acquisition will enable more than 1,000 financial institutions to access a broad range of consumer identity and authentication solutions directly from Prove

New York, NY, (July 29, 2020) – Prove (formerly Payfone), the modern platform for continuous identity authentication, today announced the acquisition of mobile authentication lines of business from Early Warning Services, LLC, a consortium owned by seven of the country's largest banks.The acquisition includes Early Warning's mobile authentication business, Early Warning's multi-factor authentication and orchestration solutions, and the Authentify® line of business.

Read More on prove.com

TechCrunch reporter Ingrid Lunden covered the news of our $100 million funding round led by Apax Digital in an exclusive last week.

"As an increasing number of daily and essential services move to digital platforms — a trend that's had a massive fillip in the last few months — having efficient but effective ways to verify that people are who they say they are online is becoming ever more important," Lunden writes. "Now, a startup called Payfone, which has built a B2B2C platform to identify and verify people using data (but no personal data) gleaned from your mobile phone, has raised $100 million to expand its business."

Lunden also notes that the market for authentication and verification services is projected to grow to $12.8 billion by 2024, according to MarketsandMarkets. She goes on to explain that while "there seems to be an almost infinite amount of variations, approaches and companies offering services to carry out the work… there's also a push to develop more seamless and user-friendly, and essentially invisible, approaches, and that's where Payfone sits."

Lunden also highlights that Payfone's commitment to and focus on protecting users and their data privacy has been a differentiator and has helped it stand out to investors.

Read the full article at TechCrunch

Investment Will Accelerate Privacy-First Customer Identity Platform with Strategic Acquisitions

New York NY, June 18, 2020 – Payfone announced it has raised $100 million to acquire strategic assets, further strengthen its machine learning capabilities, and build a cross-industry consortium to secure digital transactions and experiences. The investment was led by funds advised by Apax Digital, the growth equity team of Apax Partners.

Payfone is setting a new standard for digital identity verification and authentication. Its customer identity platform enables the world's largest financial institutions, healthcare organizations and technology companies to bring speed and security to their onboarding, digital servicing and call center processes.

Payfone's authentication solutions, including its unique Trust Score™ tool, are built on ten years of proprietary phone intelligence that enable Payfone to anonymously measure a phone number's reputation and risk with real-time processing of behavioral signals. Payfone's platform instantly detects burner phones, spoofed calls, real-time SIM swap fraud, and synthetic identities, while removing friction from legitimate transactions. Payfone also provides call verification solutions that run passively in the background of a phone call, allowing faster issue resolution.

Rodger Desai, CEO of Payfone, said, "The mobile phone is rapidly becoming the secure passport for navigating our digital lives. With one in three US consumers already authenticated by Payfone, this investment accelerates our ability to set the standard for the authentication process. As we build out a cross-industry consortium, more enterprises will be able to access Payfone's real-time fraud and risk signals to prevent account takeovers while passing more transactions."

Daniel O'Keefe, Managing Partner of Apax Digital said, "Identity is the key enabling technology for the next generation of digital businesses. Payfone's Trust Score™ is core to the real-time decisioning that enterprises need in order to drive revenue while thwarting fraud and protecting privacy."

Zach Fuchs, Principal of Apax Digital added, "Payfone's technology enables frictionless customer experience, while curbing the mounting operating expense caused by manual review." Concurrent with the investment, Mr. O'Keefe and Mr. Fuchs will join Payfone's board of directors.

Joining the investment round are new investors Sandbox Insurtech Ventures and Ralph de la Vega, the former Vice Chairman of AT&T. Existing investors MassMutual Ventures, Synchrony, Blue Venture Fund, Wellington Management LLP, and former CEO of LexisNexis Andrew Prozes also participated.

For more information about Payfone's suite of identity verification and authentication solutions, visit payfone.com.

About Payfone

Payfone is a rapidly growing software and data analytics company based in New York. Payfone's customer identity platform secures the digital experiences of the banking, insurance, telecommunication, retail, and healthcare industries. Its patented Trust Score™ enables enterprises to pass more digital transactions while thwarting fraud attacks. For the latest updates follow us at https://www.linkedin.com/company/payfone.

About Apax Digital

The Apax Digital Fund specializes in growth equity and buyout investments in high-growth enterprise software, consumer internet, and technology-enabled services companies worldwide. The Apax Digital team leverages Apax Partners' deep tech investing expertise, global platform, and specialized operating experts, to enable technology companies and their management teams to accelerate the achievement of their full potential. Over its more than 40-year history, Apax Partners has raised and advised funds with aggregate commitments of over $50 billion. These funds provide long-term equity financing to build and strengthen world-class companies. For more information see: www.apax.com

Media Contacts:

For Payfone

Emily Riley | +1 914-330-1128 | pr@payfone.com

For Apax Digital

USA Media: Todd Fogarty, Kekst CNC | +1 212-521-4854 | todd.fogarty@kekstcnc.com

UK Media: Matthew Goodman / James Madsen, Greenbrook | +44 20 7952 2000 | apax@greenbrookpr.com

Digital Identity Technology Company Achieves Dramatic Growth with Innovative Offerings

New York, April 9, 2020 – Payfone, a leader in identity verification and authentication, announced today that the Financial Times has named the company in the top 500 of The Americas' Fastest Growing Companies 2020. This is the first time FT is publishing this list for The Americas, which is focused on companies that offer impressive innovation and growth in the region.

"The inaugural FT Americas ranking comes at a perilous and uncertain time for many companies, as the coronavirus severely curtails economies, workforces and ultimately growth," said Maxine Kelly, Commissioning Editor, Special Reports at Financial Times.

"Yet the ranking also highlights 500 businesses across the continent for whom innovation and creativity have paid off — attributes that will underpin resilience and enable many of them to thrive once the worst effects of the pandemic are behind them."

Payfone, which helps its enterprise clients to secure and streamline their customer journeys through Phone Intelligence-based identity verification, ranked #4 among companies in its category and #127 overall on the list of 500 companies. The global company, which experienced 596-percent growth from 2015 to 2018, attributes its rapid growth rate to its unique technology and patents, which enable companies to solve a number of challenges across mobile, web, and call center channels. Two examples that are particularly relevant today are the company's call center ANI match technology, which significantly reduces call wait times, and its telehealth optimization solution, which helps telemedicine companies to accelerate sign-ups and logins for new and returning healthcare consumers while improving their privacy and security.

Although the award focuses on the Americas, Payfone's international solutions, such as its anti-SIM swap fraud and PSD2 SCA technologies, which are available in the United Kingdom and other European countries, were a major factor in driving its global growth.

"It is an honor to be recognized for our growth and innovation in the Financial Times' inaugural list for the Americas," said Rodger Desai, CEO of Payfone. "As digital and phone transactions surge, the need for fast and secure identity verification has become even more vital. We are committed to helping companies prioritize and accelerate their plans to optimize their online and call center experiences to offer their customers the best possible service, even in challenging times."

The Americas' Fastest Growing Companies 2020 is a joint project by the Financial Times and Statista. The results were achieved by conducting months of research, public calls, intensive database research and directly contacting tens of thousands of companies. The final list recognizes the Top 500 companies in the Americas that have achieved the highest compound annual growth in revenues between 2015 and 2018.

About Payfone
Payfone's award-winning Phone Intelligence technology replaces traditional identity verification processes such as easy-to-forget passwords, cumbersome security questions, and clumsy SMS OTPs with a solution that is both more secure and easier for end-users. Through Phone Intelligence and its patented Trust Score™, Payfone is able to verify consumers' identities in an instant, invisible, and inclusive way across mobile,

web, and call center interactions. Payfone serves the majority of US financial institutions, and leading healthcare, insurance, technology and retail companies. Learn more at payfone.com and linkedin.com/company/payfone.

Press Contact:

Emily Riley
eriley@witstrategy.com
914-330-1128

ANI trolling (also known as ANI trawling) is an emerging fraud vector that involves fraudsters running thousands of spoofed phone numbers through a business's IVR (interactive voice response) system in order to identify which numbers belong to customers of that business. Once the hackers have identified which numbers belong to customers, they launch targeted SMS phishing or smishing attacks on the individuals who own those numbers.

How ANI trolling/ANI trawling works:

When a consumer dials into a call center, it's common for a call center to try and recognize/match the ANI (automatic number identification) of the caller. If the ANI is recognized, indicating that the number is on file as belonging to a customer, the caller can be given a "green path/fast lane". If not recognized, the caller is taken down another, more generic path (typically security questions).

Armed with the knowledge about how this works, fraudsters will run thousands of numbers through a given IVR. In the process of doing that, they can identify which numbers belong to customers (based on the path that each number is routed through). When they've identified the numbers that belong to customers, they can then take those numbers and buy personal data (name, address, SSN, DOB, etc.) on the black market for them in order to run targeted smishing attacks.

How Payfone helps protect IVRs against ANI trolling/ANI trawling:

Instead of using ANI matching as a decision point, call centers can use Payfone's ANI match + call authentication to detect whether a call is being spoofed. Then they can set up the decision path such that spoofed calls always go down the generic path, regardless of whether the ANI is matched or not. That way, fraudsters can't identify which numbers belong to customers/account holders, and therefore cannot carry out SMS phishing attacks on those individuals.

Want more info about how Payfone prevents ANI trolling? Get in touch with us below to learn more.

First Name* Last Name*

Business Email*

Job Title

Phone number (optional)

Request More Info

By now, you might already know that SIM swap fraud is a major problem that can't be ignored. It's on most fraud executives' radars, not to mention in the news nearly every other week. According to the Wall Street Journal, investigators say they know of more than 3,000 SIM-jacking victims, accounting for $70 million in losses nationwide (the real numbers are likely much higher considering that many cases go unreported).

Congress is also getting involved to battle this epidemic. Earlier this month, Senator Ron Wyden published a letter to FCC chairman Ajit Pai calling on him to take action to protect consumers against number porting (a.k.a. SIM swap) scams. In Canada, the CRTC also issued a similar letter to the Canadian Wireless Telecommunications Association echoing these concerns. On top of all this, Princeton just released a study finding that top U.S. mobile carriers were vulnerable to SIM swapping tactics.

Now you know that SIM swap fraud is a serious threat to you, your company, and your customers.

What you might NOT KNOW is that there is an effective, easy-to-implement way to prevent SIM swap fraud that also improves the customer experience.

A different way of looking at SIM swap fraud

The focus of the Princeton study, Senator Wyden's letter, and really most of what has been written on the internet about SIM swap fraud has been the role that mobile carriers play in attackers carrying out fraud. As evidenced in these writeups, the step where hackers dupe customer service agents into swapping their SIMs is vital to the attack being successful. But it's also very difficult to prevent because it involves humans, and specifically customer service agents, who are trained to be as helpful as possible. But upon further inspection, this step is not where the actual damage is done.

In most cases, the actual damage – theft of funds, hijacking of a social media account, or theft of cryptocurrency – occurs *after* the fraudster actually goes to log into the victim's accounts using the phone number he has just taken over. So technically, just taking over your phone number is not enough. In order to really inflict damage, a fraudster also needs to log into your accounts.

An opportunity to stop SIM swap fraud in its tracks

This is where Payfone's patented Phone Intelligence comes into play. When the fraudster goes to log into the victim's account, the business (whether it be a bank, crypto platform, social media platform, or other kind of enterprise) can use Phone Intelligence to detect that a SIM swap has taken place and block the fraudster from taking nefarious actions.

Consider this scenario involving a cryptocurrency exchange:

1) Fraudster steals username/password of victim and logs into cryptocurrency exchange.
2) Fraudster takes over victim's phone number through a SIM swap attack.
3) With Payfone enabled, the cryptocurrency exchange can call our APIs to see if a SIM swap has occurred on that account.
4) If a SIM swap has occurred, the cryptocurrency exchange routes the user to further inspection before granting them access to the account.
5) Because accounts can be locked before any damage can be done, the cryptocurrency exchange is able to shut down hackers before they can do harm, safeguarding their users' cryptocurrency.

Why CX and digital executives should also take note

From a customer experience standpoint, Phone Intelligence has the additional benefit of creating a more seamless experience for legitimate users. Since many SIM swaps are legitimate (in 2018, there were 90 million ports and 100 million device upgrades in the U.S.), simply detecting SIM swaps and hitting anyone who has swapped their SIM with a ton of friction can be significantly damaging to your customers' experience and, in turn, customer satisfaction. Enterprises must be careful not to slow down the experience for customers who may have legitimately ported their numbers or upgraded their devices. By analyzing the contextual behavior and time of a SIM swap, Payfone provides a more sophisticated and nuanced approach to thwarting SIM swap fraud. As a result, you can offer a faster and easier experience for good customers while identifying potential bad actors and subjecting them to further inspection.

It's also important to note that customers of businesses who do not use Payfone have to jump through considerable hoops if they want to go the DIY route to protect themselves against SIM swap fraud. There are numerous articles that give recommendations on how to do this (calling your mobile carrier, setting up a pincode, then setting up a longer 16-digit pincode, etc.) but not only is this time-consuming, these precautions are totally ineffective when hackers break directly into telecom companies to swap SIMs.

The Bottom Line: Implementing technology that not only safeguards your customers against SIM swap attacks but also betters their experience is an investment. However, it's an investment that can not only help you avoid losing customers, but also to attract new customers by differentiating your company as one that cares about their security, convenience, and experience.

Want to learn more about protecting your company against SIM swap fraud while also improving your customer experience? Request a free consultation below.

First Name* ______________ Last Name* ______________

Business Email* ______________

Phone number (optional) ______________

Give us more specifics about how we can help you. (optional)

Request SIM Swap Consultation

Payfone is a proud sponsor of the 2020 Hack@CEWIT hackathon at Stony Brook! Hosted by the Center of Excellence in Wireless and Information Technology (CEWIT), this year's hackathon will see over 150 regional hackers battle it out for over $5K in prizes for the most innovative security, health-care, machine learning, A.I., blockchain, social impact, and IoT projects. The hackathon takes place February 14-16, and is open to college undergrad and grad students.

The event will also be open to the public on Sunday, Feb. 16 from 10:30am – 12pm, so come by and say hello! Visit the CEWIT site to register.

Heading to San Francisco for RSA? Use the form below to meet with us at the show to discuss how and why your fraud mitigation technology should also be improving your customer experience. And be sure to join Payfone CEO Rodger Desai as he takes the stage at eFraud Global Forum.

eFraud Global Forum: The Key to Thwarting Advanced Fraud Attacks While Improving CX
Speaker: Rodger Desai, CEO, Payfone
Date: Monday, February 24, 2020

Use the form below to set up a meeting with us at the show.

First Name* Last Name*

Business Email*

Phone number
(optional)

Is there a specific date and time that would work best for you?
(optional)

Is there a specific area or use case that you'd like to learn more about?
(optional)

Request Meeting at RSA 2020

Heading to Washington, D.C. for Health Datapalooza 2020? Join our VP of Healthcare Strategy, Mike Bechtel, as he takes the stage to share insights about how healthcare organizations can increase contactability and engagement in a HIPAA-compliant, privacy-first manner through Payfone's tokenized identity solutions.

Talk info:
HDP Rapid Fire: Ensuring Data Privacy and Security
Session: Stop the Tug of War between Delivering Great Member Experiences, Privacy and Security
Speaker: Mike Bechtel, MHSA, FACHE, Payfone
Date: Tuesday, February 11, 2020
Time: 12:45-2:00pm
Location: Marriott Marquis, Washington, D.C.

Interested in learning how you can boost engagement with your healthcare consumers in a private way that enhances their experiences? Use the form below to set up a meeting with us at the show.

First Name* Last Name*

Business Email*

Phone number (optional)

Is there a specific date and time that would work best for you?
(optional)

Is there a specific area or use case that you'd like to learn more about?
(optional)

Request Meeting at Health Datapalooza

prove
Formerly Payfone

Home
Trust Platform
Products

Company
Resources
Press and News

Contact Us
Careers Now Hiring

Privacy Policy Exercise Your Rights Do Not Sell My Personal Information

Exhibit 16

TRUSTID AUTHENTICATOR SERVICES AGREEMENT

This Services Agreement, together with the exhibits thereto listed below (this "Agreement") effective as of May 24, 2017 (the "Effective Date"), is entered into between Payfone, Inc., a Delaware corporation, (on behalf of itself and its affiliates that will participate in the relationship contemplated by this Agreement ("Payfone") with offices located at 245 5th Avenue, 11th Floor, New York, NY 10016, and TRUSTID, Inc., a Delaware corporation ("TRUSTID"), with offices at 4500 Kruse Way, Suite 350, Lake Oswego, Oregon 97035.

EXHIBITS
Exhibit A – Description of Services
Exhibit B1 –Statement of Work-AXA
Exhibit C – Support Services
Exhibit D – Service Level Agreement – Service Credits and Root Cause Analyses
Exhibit E – Compliance with Data Protection Laws and Regulations
Exhibit F – Insurance Schedule

1. SERVICES

1.1. **Services**. TRUSTID shall furnish Services, generally described in Exhibit A, ("Services") to Payfone and Payfone's Affiliates in accordance with and subject to the terms and conditions of this Agreement and one or more Statements of Work executed by the parties thereto. In the event of any discrepancy between the provisions of this Agreement and a Statement of Work, the provisions of the Statement of Work shall be controlling with respect to the relationship contemplated by that Statement of Work. Payfone may request TRUSTID to provide Services to its Affiliates, in which case, TRUSTID shall use reasonable commercial efforts to provide such Services; however, Payfone shall remain responsible for its and its Affiliates' performance under this Agreement unless TRUSTID otherwise agrees in writing. For purposes of this Agreement, "Affiliate," means any entity that controls, is controlled by, or is under common control with a party.

1.2. **Services for Resale**. The parties contemplate that Services may be provided under this Agreement for the benefit of third parties to whom Payfone may resell such Services (each a "Customer and, collectively, "Customers"). Services may be provided to Customers through direct interfaces between TRUSTID and the Customer or to Payfone for retransmission to the Customer via its interfaces with the Customer. In the event of a direct connection between TRUSTID and a Customer, the parties shall work with the Customer to provide all necessary support for the development, testing and implementation of an appropriate interface. In any such circumstance, the parties and Customer may execute such additional agreements as may be necessary or appropriate in the context of the contemplated relationship.

1.3. **Required Resources**. Each party shall provide at its expense, and shall permit the other party reasonable access to, all resources reasonably required to permit the provision of Services as contemplated in this Agreement and the applicable Statement of Work including, without limitation, information, data, communications facilities, personnel, hardware, software and other equipment. In general, and except as otherwise expressly provided in the applicable Statement of Work, the provision, operation and maintenance of resources located at the offices of a party are the responsibility of that party. In the event of any issue as to responsibility for any required resources, the parties shall negotiate in good faith a resolution of the issue, which shall be reflected in an amendment of the applicable Statement of Work. Each party shall maintain all of their respective hardware, software, systems, networks, technologies, and other assets used in providing or receiving the Services (including leased and licensed assets) in good condition.

1.4. **Standards of Performance**. In providing the Services, TRUSTID shall comply with the provisions of Exhibits C, D and E as such Exhibits may, from time to time, be modified by written agreement of the parties.

2. TERM

The Initial Term of this Agreement shall commence on the Effective Date and shall continue in effect until terminated as provided in Section 12.

3. COMPENSATION

3.1. **General**. TRUSTID shall invoice Payfone for Services and Payfone shall pay to TRUSTID the fees and charges set forth in the applicable Statement of Work (the "Fees"). Should Payfone or a Customer request additional assistance not specified in the applicable Statement of Work, the parties will negotiate an appropriate charge relating to such additional assistance, which may include reimbursement of out-of-pocket costs incurred by TRUSTID in the performance of such additional assistance and appropriate fees for professional services.

3.2. **Invoice Date**. TRUSTID shall prepare and transmit to Payfone invoices reflecting the Fees for Services and any additional assistance rendered to Payfone during the previous month by the 5th working day of the month.

3.3. **Payment Date**. All invoices shall be due and payable 30 days from the date of the invoice (the "Due Date"). A service charge of 1.5% per month may be applied to all amounts owed by Payfone to TRUSTID after their Due Date. All invoices and payments shall be in US dollars. If any amount due to TRUSTID hereunder remains unpaid 90 days after its Due Date, TRUSTID may, upon five days' notice, cease all work until payment in full is received unless, prior to the expiration of such five-day period, Payfone has provided TRUSTID with a Dispute Notice as provided in Section 3.4 or paid the outstanding amount.

3.4. **Disputed Payments**. If Payfone has reasonable basis to dispute any of the amounts set forth in any invoice rendered by TRUSTID hereunder, Payfone shall provide TRUSTID, within 45 days following the receipt of invoice, a written statement of the basis of the dispute in reasonable detail (the "Dispute Notice"). The parties agree to negotiate in good faith for the purpose of attempting to resolve such dispute. In the event such dispute is mutually agreed upon and resolved, Payfone will pay the amount so agreed by the later of ten days from the date of such agreement or the Due Date, or TRUSTID will issue a credit memo on the next invoice to Payfone (as applicable). In the event that a dispute is not resolved within sixty days following TRUSTID's receipt of the Dispute Notice despite the good faith efforts of the parties, the parties shall have the right to submit such dispute to the dispute resolution process set forth in this Agreement.

3.5. **Taxes**. Payfone shall pay all taxes and other governmental assessments, however designated (excluding taxes based upon TRUSTID's income) imposed on or based upon the provision of Services or additional assistance hereunder. If any such taxes or assessments are required to be collected and/or paid by TRUSTID, then Payfone agrees to reimburse TRUSTID for such taxes or assessments.

4. RECORD KEEPING AND AUDIT RIGHTS

4.1. **Record Keeping**. During the Term, TRUSTID shall keep or cause to be kept complete and accurate accounting records to substantiate TRUSTID's charges hereunder. TRUSTID shall maintain complete books and records (specifically including, without limitation, the originals or copies of documents supporting entries in the books of account) relating to all Services, the Statements of Work, and of all costs and fees reimbursable or payable by Payfone under the terms of this Agreement. TRUSTID shall retain all such books and records during the Term and for a period of one year thereafter, but in no event longer than five years from the date of the record.

4.2. **Party Audit Rights**. During the Term and for a period of one year thereafter, Payfone shall, upon reasonable prior notice, have the right to examine, or to have its representatives examine, and audit such books and records at any reasonable time during that period but no more than once during any rolling twelve-month period unless Payfone shall have reason to believe that there exists a material discrepancy in such books and records. TRUSTID shall credit any overcharges to Payfone on Payfone's next monthly invoice. The costs associated with any such audit shall be borne by Payfone unless such audit demonstrates that TRUSTID's charges during the period subject to the audit exceeded the proper and accurate amount of such charges pursuant to this Agreement by ten percent or more, in which case TRUSTID shall reimburse Payfone for all reasonable costs associated with the audit, and shall reimburse Payfone for all overpayments. If any such audit demonstrates an undercharge, Payfone shall promptly pay TRUSTID the amount of the undercharge, without interest.

4.3. **Governmental Audit Rights**. Each party will cooperate in all reasonable respects with any investigation, audit or other proceeding legitimately undertaken by a governmental agency or private body authorized by the government to perform such functions in connection with its oversight of the other party.

5. RELATIONSHIP MANAGEMENT

5.1. **Payfone Project Manager**. Payfone will appoint and, at all times during the Term, maintain a project manger (the "Project Manager"). The Project Manager shall be responsible for managing Payfone's participation in the delivery of the Services, and shall be authorized to act as Payfone's primary contact for TRUSTID under this Agreement. The Project Manager will have authority to resolve all issues relating to this Agreement unless the consent of another person is required by law, under Payfone's charter documents or by resolution of Payfone's Board of Directors. The Project Manager shall serve as the primary contact person for the resolution of any disputes arising under this Agreement, or with provision of Services. The Project Manager may be replaced at any time upon written notice to TRUSTID.

5.2. **Key TRUSTID** Personnel. TRUSTID shall at all times provide adequate qualified personnel to provide the Services.

6. PUBLICITY

TRUSTID may not reference Payfone or its relationship with Payfone in any communications to third parties (other than third parties involved in the performance of TRUSTID's obligations under this Agreement or as may be required by law); provided, however, TRUSTID may, with prior written consent, include Payfone's name along with its properly formatted logo in lists of TRUSTID customers in marketing materials, including the TRUSTID web sites and as otherwise required by applicable law, regulation or court order.

7. CONFIDENTIAL INFORMATION; INTELLECTUAL PROPERTY

7.1. **Confidentiality**. The parties expect to disclose, each to the other Confidential Information. Each party hereto shall hold in confidence all Confidential Information of the other party using the same level of care used to protect its own confidential information, but no less than reasonably prudent care. "Confidential Information" is information (i) as to which the disclosing party has a proprietary interest or a legal or contractual obligation to protect the proprietary interest of a third party, (ii) that the disclosing party maintains in confidence, or (iii) that is of a nature that the receiving party should reasonably understand to be confidential or as to which the receiving party has been notified that the disclosing party treats it as confidential. Confidential Information includes, without limitation, information related to the disclosing party's products, services, customers and methodologies, or to its research and development, trade secrets or business affairs. Confidential Information does not include (i) information which is or becomes a matter of public knowledge through no fault of the receiving party; (ii) information which is or becomes known to the receiving party from third parties who in making such disclosure breach no confidentiality obligation to the disclosing party; or (iii) information that the receiving party can demonstrate by clear and convincing evidence was independently developed by it or its Affiliates, consultants or vendors without reference to any Confidential Information of the disclosing party. Confidential Information may be disclosed in response to a valid order of a court, regulatory agency or other governmental body, but only to the extent of and for the purposes stated in such order; provided, however, that the receiving party shall, unless prohibited from doing so by law, first notify the disclosing party in writing of the order and cooperate with the disclosing party if the disclosing party desires to seek an appropriate protective order.

7.2. **Disclosure and Use of Confidential Information.** Neither party may use the other party's Confidential Information except as contemplated by this Agreement and the applicable Statement of Work. A receiving party may disclose Confidential Information of the disclosing party to its employees, consultants, subcontractors, attorneys, auditors and members of its Board of Directors, in each case (i) to the extent that such disclosure is reasonably necessary in connection with the provision of Services or otherwise in the conduct of the legitimate duties of such persons, and (ii) provided that such persons are parties to agreements similar in scope to the provisions of this Section 7 or are otherwise under a comparable legal obligation with respect to any Confidential Information so received. Promptly upon becoming aware thereof, the receiving party shall report to the other party any breach of the confidentiality provisions of this Agreement. Payfone shall not, without the prior written approval of TRUSTID, disclose TRUSTID Confidential Information to a Customer.

7.3. **Pre-Existing Intellectual Property**. Each party shall retain ownership of all right, title and interest in and to any intellectual property it owned or had an interest in prior to the Effective Date, including, but not limited to all copyright, patent, trademark, service mark and trade secret rights, technical documents, technical data, documentation and engineering materials (collectively, the "Pre-existing Intellectual Property"). Unless expressly stated herein or in the Statement of Work, nothing in this Agreement shall be deemed to imply a transfer of ownership of the Pre-existing Intellectual Property.

7.4. **Developed Intellectual Property**. Unless otherwise agreed in writing, any and all intellectual property developed during the Term and relating to the Services shall remain the property of the party that developed it. Intellectual property jointly developed by the parties in connection with the Services shall be owned as described in a written agreement between the parties and otherwise shall be owned fully and jointly by each party with full right of use and assignment.

7.5. **License for the Purpose of this Agreement**. TRUSTID hereby grants to Payfone a license to use, during the Term and solely for the purposes contemplated by this Agreement, any and all of its intellectual property as reasonably necessary in connection with the provision of Services.

8. INDEMNIFICATION

8.1. **TRUSTID Indemnification**. TRUSTID will indemnify, defend and hold Payfone (and its employees, officers, directors and agents) harmless from all claims, damages, liabilities, losses, costs and expenses (including without limitation reasonable attorneys' fees) arising out of or resulting from any third party claim, action or other proceeding (including any proceeding by any of TRUSTID's employees, officers, directors, agents or customers) that is based upon or relates to TRUSTID's infringement or misappropriation of any patent, copyright, trade secret, trademark or other intellectual property right in connection with the provision of Services to Payfone; provided, however, that TRUSTID will have no liability for claims of infringement arising from (i) any alteration or modification to the software not performed by or at the direction of TRUSTID, (ii) alterations or modifications to intellectual property in accordance with Payfone's written requirements, where the infringement is due to such requirements, or (iii) the combination, operation or use of its technology with third party technology not provided by TRUSTID. TRUSTID's indemnification obligations are contingent upon Payfone's prompt notification of any claim or potential claim for which it may seek indemnification. Payfone shall provide TRUSTID with the opportunity to control the defense of such claim and the information and assistance necessary to provide such defense, at TRUSTID's expense. Payfone may, at its option and sole cost, participate in the defense in any such proceeding.

8.2. **Payfone Indemnification**. Payfone will indemnify, defend and hold TRUSTID (and its employees, officers, directors and agents) harmless from all claims, damages, liabilities, losses, costs and expenses (including without limitation reasonable attorneys' fees) arising out of or resulting from any third party claim, action or other proceeding (including any proceeding by any of Payfone's employees, officers, directors, agents or customers) that is based upon Payfone's knowing infringement or misappropriation of any patent, copyright, trade secret, trademark or other intellectual property right in connection with the provision of Services; provided, however, that Payfone will have no liability for claims of infringement arising from (i) any alteration or modification to the software not performed by or at the direction of Payfone, (ii) alterations or modifications to intellectual property in accordance with TRUSTID's written requirements, where the infringement is due to such requirements, or (iii) the combination, operation or use of its technology with third party technology not provided by Payfone. Payfone's indemnification obligations are contingent upon TRUSTID's prompt notification of any claim or potential claim for which it may seek indemnification.

TRUSTID shall provide Payfone with the opportunity to control the defense of such claim and the information and assistance necessary to provide such defense, at Payfone's expense. TRUSTID may, at its option and sole cost, participate in the defense in any such proceeding.

8.3. **Infringement Remedies**. If, in the reasonable opinion of a party providing technology used in connection with the provision of Services, any such technology infringes or is likely to infringe the proprietary rights of any third party, such party may elect to secure the right to continue using the technology or to replace or modify the technology to the extent required to cause it to be non-infringing. In any such event, this Agreement shall continue in full force and effect unless the replacement or modification materially impairs the value of the Services to Payfone, in which case Payfone may elect to cause the Term to end following ten days prior written notice. If any infringement or likely infringement as described in this Section 8.3 causes the cost to TRUSTID of providing the Services to be materially increased, the parties shall negotiate in good faith an appropriate amendment to the related Statement of Work.

9. PAYFONE RESPONSIBILITIES

9.1. **Access to Equipment**. Payfone agrees to provide promptly and permit reasonable electronic access to Payfone equipment and resources, subject to Payfone's customary security and safety requirements, and to provide the necessary environment for such equipment and resources as is necessary for TRUSTID to provide the Services.

9.2. **Business Requirements**. Payfone shall be responsible on a continuing basis for advising TRUSTID of the requirements and nature of Payfone's business as they may affect the provision of the Services.

9.3. **Provision of Information**. Payfone shall provide in a timely manner all such information, data, requirements or specifications that are reasonably required in connection with the provision of Services.

10. WARRANTIES

10.1. **Performance of Services**. TRUSTID represents, warrants and covenants that the Services shall be those described in the Statement of Work and shall be provided in a professional and workmanlike manner.

10.2. **Nature of Services**. TRUSTID's AUTHENTICATOR assesses the usability of calling party numbers (ANIs) for authentication as defined in Exhibit A Description of Services.

10.3. **Support Services**. TRUSTID provides Support Services as defined in Exhibit C Support Services.

10.4. **No Default/Conflict**. TRUSTID and Payfone each represents and warrants to the other that its signing, delivery and performance of this Agreement shall not constitute a violation of any judgment, order or decree or a material default under any material contract by which it or any of its material assets are bound. TRUSTID and Payfone each further represents and warrants that the execution and performance of this Agreement by it shall not violate any law, statute or regulation and shall not conflict with or breach any agreement, covenant, court order or decree to which it is a party or by which it is bound, whether in effect as of the Effective Date or entered into thereafter.

10.5. **Authorization**. TRUSTID and Payfone each represents and warrants to the other that (i) it has the requisite corporate power and authority to enter into this Agreement and to carry out the transactions contemplated by this Agreement; and (ii) the signing, delivery and performance of this Agreement and the consummation of the transactions contemplated by this Agreement have been duly authorized through all requisite corporate action.

10.6. EXCEPT FOR THE WARRANTIES STATED IN THIS AGREEMENT, TRUSTID DISCLAIMS ALL EXPRESS OR IMPLIED WARRANTIES WITH REGARD TO THE SERVICES FURNISHED UNDER THIS AGREEMENT, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

11. INSURANCE

At all times at which TRUSTID is providing Services under this Agreement it shall maintain in full force and effect the policies of insurance listed in Schedule E.

12. TERMINATION

12.1. **Termination for Unlawfulness**. Either party may terminate this Agreement at any time without prior notice if and to the extent such termination is necessary to prevent the violation, or the continuation thereof, by the terminating party of any law, rule, regulation or competent order of any court or governmental body applicable to it; provided that the terminating party shall provide prompt written notice to the other party of any such termination, stating in reasonable detail the reasons therefor.

12.2. **Termination for Default**. In the event of a Default, the non-defaulting party shall have the right to terminate this Agreement effective at 11:59 p.m. on a termination date specified by the non-defaulting party in a termination notice specifying in reasonable detail the nature of the alleged default and sent to the defaulting party not less than thirty days prior to the specified termination date, provided that the defaulting party has not cured such default within such thirty-day period. Termination shall not constitute the terminating party's exclusive remedy for such Default, and the terminating party shall not be deemed to have waived any of its rights accruing hereunder prior to such Default. The occurrence of any of the following shall be considered a "Default":

12.2.1. a material breach by either party of any obligation under this Agreement, provided that such material breach, if curable, is not cured within thirty days after the other party has received written notice of such material breach;

12.2.2. the discovery that a representation made in this Agreement by a party was knowingly false when made, if the nature and magnitude of the misrepresentation are such that they would have had a probable and material effect upon the non-defaulting party's decision to engage the other party or upon the negotiations as to the other terms of this Agreement; or

12.2.3. a judicial declaration of the insolvency of a party; the general failure of a party to pay its debts in the normal course of business; the entrance of a party into receivership or any arrangement or composition with creditors generally; the filing of a voluntary or involuntary petition that is not dismissed within 60 days for the bankruptcy, reorganization, dissolution or winding-up of a party; a general assignment for the benefit of creditors of a party; or a seizure or a sale of a material part of a party's property by or for the benefit of any creditor or governmental agency.

12.3 **Termination by Customer.** Customer may terminate this Agreement at any time by providing at least 30 days' written notice to TRUSTID.

12.4 **Scope of Termination.** Each SOW will have the term set forth therein, provided that, unless otherwise agreed by the parties in writing, each SOW will terminate automatically upon termination of the Agreement.

12.5 **Effect of Termination.** Upon termination of this Agreement, unless the parties otherwise agree, the provision of Services shall cease and no further Services shall be provided hereunder. Following termination: (i) TRUSTID shall remain entitled to payment for Services provided and (ii) provisions relating to conduct of the parties that can reasonably be understood to survive termination, including, but not limited to, the provisions of Sections 4, 7, 8, 10, 13 and 15 through 25 shall continue in effect.

13. LIMITATION OF LIABILITY

EXCEPT IN THE CASE OF FRAUD OR WILLFUL MISCONDUCT, EACH PARTY'S TOTAL LIABILITY FOR LOSS, DAMAGE OR EXPENSE IN CONNECTION WITH OR ARISING FROM THIS AGREEMENT SHALL BE LIMITED TO DIRECT DAMAGES PROVEN, AND NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES OF ANY KIND, NOR FOR LOSS OF PROFITS, LOSS OF REVENUE, BUSINESS OR GOODWILL, UNDER OR ARISING OUT OF THIS AGREEMENT, HOWEVER CAUSED.

14. WORK RULES, RELATIONSHIP OF THE PARTIES

14.1. **Work Rules**. It is not contemplated that the provision of Services will require physical access by TRUSTID personnel to any Payfone facilities. However, should such access be necessary or desirable, TRUSTID employees and agents, while on the premises of Payfone, shall comply with all Payfone rules, regulations and policies. Each party shall be responsible for supervision and direction of the work by its employees, agents and subcontractors. TRUSTID shall, at its sole expense, comply with Payfone's reasonable requests regarding background checks for personnel providing Services.

14.2. **Relationship of the Parties**. This Agreement shall not be construed to create a relationship in which either party is a representative, agent, employee, partner or joint venturer of the other. TRUSTID shall be an independent contractor for the performance under this Agreement. Neither party shall have the authority to enter into any agreement, nor to assume any liability, on behalf of the other party, nor to bind or commit the other party in any manner, except as provided hereunder. Each party's employees and subcontractors who perform under this Agreement shall remain employees and subcontractors of that party and each party shall have sole responsibility for such employees and subcontractors, including responsibility for payment of compensation to such personnel and for injury to them in the course of their employment. Each party shall be responsible for all aspects of labor relations with such employees and subcontractors, including their hiring, supervision, evaluation, discipline, firing, wages, benefits, overtime and job and shift assignments and all other terms and conditions of their employment, and the other party shall have no responsibility therefor. Notwithstanding the use of subcontractors by either party, each party shall remain liable under this Agreement for its subcontractors' performance.

15. COMPLIANCE WITH LAWS

TRUSTID shall comply with all federal, state and local laws, ordinances, rules, regulations and orders applicable to TRUSTID with respect to its performance of the Services, and obligations under this Agreement. Payfone will comply with all federal, state and local laws, ordinances, rules, regulations and orders applicable to Payfone with respect to its obligations under this Agreement.

16. DISPUTE RESOLUTION

In the event any controversy, claim, dispute, difference or misunderstanding between TRUSTID and Payfone (a "Dispute") arises out of or relates to this Agreement, TRUSTID and Payfone shall designate managers to meet and negotiate in good faith in an attempt to amicably resolve the Dispute. The designated managers shall attempt to resolve the Dispute and any resolution to which they mutually agree shall be binding on the parties. If the managers are unable to resolve the Dispute through good faith negotiations within a reasonable period of time, or if either manager states in writing that the discussions are at an impasse, TRUSTID and Payfone shall promptly prepare a written position statement that summarizes the unresolved issue(s) and the party's proposed resolution. The respective position statements shall be delivered by TRUSTID to Payfone's Chief Executive Officer and by Payfone to TRUSTID's Chief Executive Officer for resolution. In the event that the Dispute is not resolved in the manner described in this Section, each party shall be entitled to pursue any and all remedies that are available to it at law or in equity.

Notwithstanding the foregoing paragraph, either party may, at any time during the pendency of the dispute resolution process described in this Section 16, apply to any court of competent jurisdiction for a stay, injunction or other temporary order that it reasonably deems necessary to protect its material interests, provided that any such application shall not affect the provisions of Section 19 with respect to jurisdiction and venue in connection with any Dispute that proceeds to litigation.

17. RETURN OF INFORMATION UPON EXPIRATION OR TERMINATION

Upon the termination or expiration of this Agreement, at the written request of either party, the other party shall promptly destroy or deliver to the requesting party all copies and embodiments in whatever form of the requesting party's Confidential Information and, if requested by the requesting party, shall provide the requesting party with written confirmation that all such materials have been returned or destroyed in accordance with appropriate industry standards. Notwithstanding the foregoing, (i) the receiving party's legal department and external legal counsel may each keep copies of the Confidential Information to the extent required by applicable law, regulation or bone fide and consistently applied document retention policy that is customary for the industries in which it or they (as the case may be) operate, and (ii) the receiving party may retain Confidential Information to the extent it is automatically "backed-up" on its or their (as the case may be) electronic information management and communications systems or servers, provided that such copies are destroyed in accordance with the receiving party's standard policy for archival copies. This Section does not release the receiving party from their obligations to keep such Confidential Information confidential.

18. ASSIGNMENT

Except as otherwise permitted in this Section 18, neither party shall assign any right or obligation under this Agreement without the prior written consent of the other party, which consent shall not be unreasonably withheld, delayed or conditioned. Any assignment without such written consent shall be void. Notwithstanding the preceding sentence, either party may assign this Agreement and its rights and obligations hereunder to a third party that agrees in writing to be bound thereby upon written notice to the other party in connection with an internal reorganization of the parent of the transferor or the transfer or sale of all or substantially all of its business. Any authorized assignment under this paragraph shall be binding upon and inure to the benefit of the parties, their respective successors (whether by stock or asset transfer or any change of control by any other means), personal representatives and permitted assigns.

19. APPLICABLE LAW AND BINDING EFFECT; JURISDICTION

This Agreement shall be governed by and construed in accordance with the laws of the State of Oregon, excluding its conflicts of law rules, and shall inure to the benefit of and be binding upon the parties hereto and their heirs, personal representatives, successors and permitted assigns. Any disputes regarding the subject matter of this Agreement shall be brought exclusively in the state or federal courts located in Multnomah County, Oregon.

20. NOTICES

All notices given hereunder will be given in writing, will refer to this Agreement and will be personally delivered, sent by registered or certified mail (return receipt requested) to the address set forth below. Either party may from time to time change such address by giving the other party notice of such change in accordance with this Section. All notices shall be deemed given as of the day they are received.

If to Payfone: 245 5th Avenue 11th Floor New York, NY 10016 Attn: Legal Department	If to TRUSTID: 4500 Kruse Way Suite 350 Lake Oswego, OR 97035 Attn: Patrick Cox, CEO

21. SEVERABILITY

If any provision of this Agreement is held invalid, illegal or unenforceable in any jurisdiction, for any reason, then, to the full extent permitted by law (a) all other provisions hereof will remain in full force and effect in such jurisdiction and will be construed in order to carry out the intent of the parties hereto as nearly as may be possible, (b) such invalidity, illegality or unenforceability will not affect the validity, legality or enforceability of any other provision hereof, and (c) any court or arbitrator having jurisdiction over this Agreement will have the power to reform such provision to the extent necessary for such provision to be enforceable under applicable law.

22. WAIVER; AMENDMENT

No delay or failure by a party hereto in exercising or enforcing any of its rights or remedies hereunder, and no course of dealing or performance with respect thereto, will constitute a waiver thereof. The express waiver by a party hereto of any right or remedy in a particular instance will not constitute a waiver thereof in any other instance. Except as expressly provided in this Agreement, no amendment, waiver or discharge of any provision of this Agreement will be effective unless made in writing that specifically identifies this Agreement and the provision intended to be amended, waived or discharged and signed by both parties.

23. HIRING OF EMPLOYEES

Each party agrees that it will not solicit for employment the other party's employees who are involved with the work relating to this Agreement during the term of this Agreement and for a period of one year following termination unless otherwise mutually agreed in writing. Notwithstanding the foregoing, neither party is prohibited from soliciting for employment the other party’s employee pursuant to a general solicitation on the part of the hiring party (by way of example only, an Internet posting, newspaper advertisement or headhunter engagement).

24. SECTION AND PARAGRAPH HEADINGS

Section and paragraph headings used throughout this Agreement are for reference and convenience and in no way define, limit or describe the scope or intent of this Agreement or affect its provisions.

25. ENTIRE AGREEMENT

This Agreement supersedes any and all prior negotiations, representations, understandings and agreements with respect hereto, and constitutes the entire agreement of the parties hereto with respect to the subject matter hereof. All attachments are incorporated into this Agreement.

The parties have executed this Agreement as of the date first set forth above.

Payfone, Inc.

By: Thomas FitzSimmons
Thomas FitzSimmons (May 25, 2017)

Name: Thomas FitzSimmons

Title: CFO

Date: May 25, 2017

TRUSTID, Inc.

By: Patrick M. Cox

Name: Patrick Cox

Title: CEO

Date: May 24, 2017

EXHIBIT A

Description of Services

Nature of Services:

TRUSTID's AUTHENTICATOR assesses the usability of calling party numbers (ANI) for authentication by Payfone. The suitability of the ANI is determined by TRUSTID using information related to the call itself, data supplied by third parties and TRUSTID's technology. TRUSTID does not receive or process telephone calls, rather data about telephone calls. TRUSTID's AUTHENTICATOR service labels each ANI with a high degree of probability, as Credentialed or as Uncredentialed, and transmits that assessment (the "Validity Code") to Payfone. The assessments are as follows:

- *Credentialed*: high probability the call originated from the indicated telephone number;

- *Uncredentialed*: call characteristics indicate that the ANI should not be used for authentication. Uncredentialed calls include (i) calls from a payphone, satellite phone, pc-based VoIP software phone, (ii) calls that have invalid numbers, have no assigned carrier, show untrustworthy network signaling or (iii) calls where errors prevent TRUSTID from making a determination.

The sole function of the Services is to assist Payfone in determining the probable authenticity of the ANIs associated with incoming calls. The Services are not designed to and do not validate the identity, integrity or creditworthiness of the caller or any other person, nor do they determine the action that Payfone should take.

Performance:

TRUSTID's AUTHENTICATOR determines the Validity Code using real-time telephone network forensics performed pre-answer, during and up to the first ten seconds of an unanswered incoming call. The total time starting from when TRUSTID receives a validation request and ending when it returns a Validity Code to Payfone shall not normally exceed ten seconds for any call.

Detectability:

TRUSTID's AUTHENTICATOR is highly undetectable on a non-spoofed caller's line. When an incoming calling party number has been manipulated, hacked, spoofed or is otherwise Uncredentialed, AUTHENTICATOR may cause the actual line associated with the spoofed or Uncredentialed number to ring once.

Implementation:

TRUSTID receives information about phone calls via an application programming interface (API) request, placed from one or more properly configured systems (a "Requesting System") and sent to TRUSTID's multiple service points. TRUSTID API requests use secure, encrypted Internet-based HTTPS protocols.

To enable implementation Payfone shall:

- Provide two or more Requesting Systems utilizing the API;

- Provide connections with sufficient throughput and speed to send and receive API traffic to and from two or more TRUSTID service points;
- Not deliver answer supervision on incoming telephone calls for which the AUTHENTICATOR service is configured until TRUSTID's Validity Code is received.
- If a TRUSTID validity code is not received after ten seconds from the sending of the API request, answer supervision may be provided and call processing may continue; and
- Not process already-answered telephone calls to any phone line where the AUTHENTICATOR service is configured.

New Payfone Projects shall use the current version of the TRUSTID AUTHENTICATOR API.

Enhancements, Upgrades and Other Changes:

TRUSTID reserves the right to make changes in its technology, its relationships with third party providers and other features of TRUSTID's AUTHENTICATOR and to implement any and all such changes in the Services as long as the Services, as so changed, continue to meet or exceed the standards set forth under Performance, above.

EXHIBIT B1

Statement of Work - AXA

This Statement of Work ("SOW") constitutes a Schedule to that certain Services Agreement (the "Agreement"), dated as of ___________, 201_, by and between TRUSTID, Inc. ("TRUSTID") and Payfone, Inc. ("Payfone"). Capitalized terms used herein and not otherwise defined have the meanings ascribed to them in the Agreement. It relates to the provision of Services to AXA Equitable Life Insurance Company ("AXA").

Nature of Project

The project contemplated by this SOW (the "Project") integrates AXA's telephony infrastructure and/or related systems and TRUSTID's AUTHENTICATOR service in order to automate authentication on AXA specified inbound phone calls. The integration contemplated in the prior sentence will be established between TRUSTID and AXA through the intermediary of Payfone.

The Project is contemplated in two parts, an Implementation Period in which AXA's telephony infrastructure is integrated Payfone and determined to be functional with acceptance testing by AXA, followed by a Service Period in which TRUSTID provides AUTHENTICATOR services to Payfone and AXA.

References

TRUSTID maintains product documentation that details AUTHENTICATOR's functionality and integration. Reference is made to the product documentation to supplement the information contained herein.

Project Assumptions

The Project is undertaken on the following assumptions:

- Payfone will develop integration to the current AUTHENTICATOR API.
- TRUSTID will advise Payfone regarding Payfone-side environments and systems required to integrate to AUTHENTICATOR. Payfone and TRUSTID will document these requirements.
- Payfone will build and maintain Payfone-side environments and systems, and will work with AXA to build and maintain AXA-side environments and systems, including the development of software, to integrate to AUTHENTICATOR.
- Payfone will configure networking to connect to all available TRUSTID data centers.
- TRUSTID will provide a pre-production environment to support testing. The pre-production environment will operate with test and production data. Payfone may also test in its lab environment.
- Payfone will be responsible for the system integration testing (SIT), as specified in the project plan to be agreed upon between TRUSTID and Payfone. Payfone shall provide updates on the testing progress and any related issues/problems.
- Payfone will be responsible for user acceptance testing (UAT) as specified in the project plan to be agreed upon between TRUSTID and Payfone. Payfone shall provide updates on the testing progress and any related issues/problems.

- Payfone will include in the information that it provides to TRUSTID pursuant to Section 9.3 of this Agreement Payfone transactional data for each request made to the AUTHENTICATOR API and the complete response delivered to AXA. The delivery of this data shall be made periodically by mutual agreement.

A. Implementation Period

Unless specified otherwise, all tasks and deliverables are to be completed by TRUSTID. The Implementation Period will consist of the following phases:

1. Software Requirements Phase

Task Summary

- Confirm the project teams' roles and responsibilities.
- Prepare a software requirements specification (SRS) of all software components for the functionality to be implemented.

Deliverable and Acceptance

- Software requirements specification
- Acceptance
  - Payfone will approve and provide written acceptance of the SRS within ten business days of receipt or propose suggested changes. TRUSTID shall answer queries from Payfone promptly and diligently; where Payfone has outstanding or ongoing queries, the ten business days may be extended by Payfone consistent with the number of days TRUSTID needs to answer Payfone's queries.
  - If TRUSTID accepts the proposed changes, TRUSTID shall update the SRS and again submit it to Payfone for Payfone's approval. If TRUSTID rejects the proposed changes or the Parties cannot agree on the SRS, the Parties shall involve senior management in a good faith attempt to reach a mutually acceptable compromise after first using an escalation process, including mediation of the dispute with representatives from executive management, then the parties have the option of submitting their claims to a court of competent jurisdiction. Upon final approval of the SRS, TRUSTID shall begin the system design.

2. Software Design Phase

Task Summary

- Prepare a detailed software design specification (SDS) of all software components per the SRS.
- Identify Payfone-side information for a successful integration, including, but not limited to, integration points, integration method, data interface specifications.

Deliverable and Acceptance

- Solution Design Specification (SDS)
- Acceptance
  - Payfone will approve and provide written acceptance of the SDS within ten business days of receipt or propose suggested changes. TRUSTID shall answer queries from Payfone promptly and diligently; where Payfone has outstanding or ongoing queries, the ten business days may be extended by Payfone consistent with the number of days TRUSTID needs to answer Payfone's queries.
  - If TRUSTID accepts proposed changes, TRUSTID shall update the SDS and again submit it to Payfone for Payfone's approval. If TRUSTID rejects the proposed changes or the Parties cannot agree on an SDS, the Parties shall involve senior management in a good faith attempt to reach a mutually acceptable compromise. Upon final approval of the SDS, TRUSTID shall begin development.

3. Development Phase

Task Summary

- Configure and implement AUTHENTICATOR as defined in the SDS.
- Configure all TRUSTID pre-production environments.
- Validate connectivity between TRUSTID and Payfone infrastructure.
- Support Payfone's unit testing activities.

Deliverable

- AUTHENTICATOR implemented per the SDS and available for system integration testing.

4. System Integration Testing (SIT) Phase

Task Summary

- Support Payfone's SIT activities.
- Correct all defects identified during SIT.
- With Payfone, complete production readiness testing (PRT).
- Correct all defects identified during PRT.

Deliverable & Acceptance

- SIT completed.
- PRT completed.
- Acceptance
  - Payfone will provide approval and acceptance of the TRUSTID solution within two weeks of the completion of SIT. TRUSTID shall answer queries from Payfone promptly and diligently; where Payfone has outstanding or ongoing queries, the two weeks may be extended by Payfone consistent with the number of days TRUSTID needs to answer Payfone queries. TRUSTID shall review all identified deficiencies. If TRUSTID accepts the identified deficiencies, TRUSTID shall update the TRUSTID software accordingly for Payfone's review to gain acceptance of the completed remediation.

5. User Acceptance Testing (UAT) Phase

Task Summary

- Support Payfone's UAT activities.
- Correct all defects identified during UAT.

Deliverable & Acceptance

- UAT completed.
- Acceptance
  - Payfone will provide approval and acceptance of the TRUSTID solution within four weeks of the completion of UAT. TRUSTID shall answer queries from Payfone promptly and diligently; where Payfone has outstanding or ongoing queries, the four weeks may be extended by Payfone consistent with the number of days TRUSTID needs to answer Payfone queries. TRUSTID shall review all identified deficiencies. If TRUSTID accepts the identified deficiencies, TRUSTID shall update the TRUSTID software accordingly for Payfone's review to gain acceptance of the completed remediation.

6. Deployment Phase

Task Summary

- Set-up and configure production environment
- Support Payfone's stress and performance testing and remediate identified issues.
- Conduct knowledge transfer sessions with Payfone.
- Identify mutual incident response and maintenance procedures inclusive of communications plan.
- Support Payfone's release plan and remediate identified issues.

Deliverables

- Stress and performance testing completed.
- Knowledge transfer sessions completed.
- Incident response procedures.
- Maintenance response procedures.
- Communications plans inclusive of NOC (Network Operations Center) contact information.
- TRUSTID AUTHENTICATOR released to production service period.

Change Control Procedure

It may become necessary to amend this SOW for reasons including, but not limited to, the following:

- Discretionary changes to the project schedule and/or scope
- Requested changes to the work hours of Payfone or TRUSTID personnel
- Non-availability of products, resources or services which are beyond Payfone's or TRUSTID's control
- Environmental or architectural impediments not previously identified

- Lack of access to personnel or facilities necessary to complete project

In the event that it is necessary to change this SOW, the following process will be followed:

- A project change request (PCR), in substantially the format set forth in SOW Exhibit 1, will be the vehicle for communicating a request for change.
- The PCR must describe the change, reasons for the change, and the effect the change will have on the project, which may include scheduling changes, pricing, etc.
- Either Payfone or TRUSTID may initiate a PCR. The designated Project Manager of the requesting party will review the proposed change and determine whether to submit the request to the other party.
- Both the TRUSTID and Payfone Project Managers will review the proposed change and approve or reject it.
- When acceptable, both parties will sign the PCR, which may affect pricing, schedules and contractual commitments.
- The SOW or Purchase Order affected by the change will be indicated on a PCR, and the PCR Number will be referenced on invoicing.
- PCRs not signed by both parties will have no force or effect.

B. Service Period

The Service Period begins following the production release of AUTHENTICATOR. TRUSTID shall provide AXA support as described in Exhibit C, “Support Services”, of the related agreement. TRUSTID provides a staffed Network Operations Center (NOC) that is available 24 hours a day, 7 days a week.

C. Termination

Payfone may terminate this SOW upon written notice to TRUSTID if AXA is not satisfied with its UAT as described above.

D. Fees and Pricing

The total Transactions sent from Payfone to TRUSTID for validation determine transaction pricing. Every phone number (ANI/Caller ID) sent to TRUSTID for validation is a Transaction.

Transaction Fees: Transaction volumes are aggregated across a Payfone’s enterprise to calculate the lowest price. Higher volumes receive lower pricing. Payfone pay a Transactions Fee for GREEN results; RED results are no cost.

*Implementation Period***:**

TRUSTID anticipates that fewer than 500 Transactions will be needed for the combined purposes of SIT, UAT and stress/performance testing during the Implementation Period and will provide up to 500 Transactions at no cost in support of testing. Any additional processed Transactions during the Implementation Period will be billed in the manner applicable to Transactions during the Service Period.

Service Period:

The fee per GREEN result is $0.10 USD

RED results will be $0.00 USD.

Transaction Fees and additional fees due are invoiced monthly.

Professional Service Fees:

The price for the Professional Services described in this SOW is $10,000. The Professional Services fees shall be invoiced upon the completion of AXA's UAT, provided, however, that AXA 1. Is satisfied with the UAT and is prepared to move forward with the Deployment Phase and 2. AXA and Payfone have signed an agreement for use of the services described in this SOW. If either condition 1 or 2 above are not met, Payfone will not owe the fee described in this paragraph and this SOW will automatically terminate.

Except as set forth below, the basis for Professional Service Fees during the Initial Term is $220 per hour.

The estimated hours of professional services required to complete the Implementation Phase are summarized in the following table:

#	Role	Estimated Baseline Hours
1	VP, Professional Services / PM	32
2	VP, Software Engineering / Developer	36
	Total	68

For the avoidance of doubt, in no event will Payfone owe more than $10,000 for Professional Services under this SOW.

SOW EXHIBIT 1
Project Change Request

TRUSTID®

General Information	
Change Request Number	
Project Name	
Client Name	
Project Manager	
Salesperson	
Target Go-Live Date	

Background and Scope of Requested Change			
Requestor		Phone	
Release		Date Prepared	
Change Title			
Change Description			
Scope			

Impact of Requested Change	
Change Assessment	
Users Impacted	
Systems Impacted	

Time and Materials *Cost of Change*	*Required Hours*	*Hourly Rate*	*Estimated Cost*
Total			
Note: Services are invoiced monthly on a Time and Materials basis. Any travel expenses will be approved by the Payfone in writing. Payment terms are consistent with those in the Services Agreement.			

Timeline		
Milestones	Original Date	New Date

Approval	
Company	
Signature	
Name	
Title	
Date	

Approval	
TRUSTID	
Signature	
Name	
Title	
Date	

EXHIBIT C

Support Services

TRUSTID will provide Payfone with the following Support Services for the Services:

1. 24 x 7 Support; Severity Levels. TRUSTID will provide Support Services on a 24 x 7 x 365 basis and will respond to service requests and correct Errors or provide a Work-Around in accordance with the severity level reasonably assigned by Payfone as follows:

SEVERITY LEVEL	RESPONSE TIME	CORRECTION TIME
Severity 1	30 minutes	Two hours
Severity 2	One hour	Four hours
Severity 3	Three hours	24 hours
Severity 4	24 hours	One week

A Severity 1 Error: (i) causes the facilities and/or software to be unavailable or cease operating in any material respect; or (ii) is likely to directly or indirectly delete, impair, damage or corrupt (collectively with (i), "Damage") System or Data. A Severity 1 Error will also include any Error that poses direct or indirect imminent harm to System or Data.

A Severity 2 Error: (i) causes a significant function of the facilities and/or software to be unavailable or impaired although it still operates; (ii) may cause Damage to any System or Data; or (iii) may have a material adverse impact on Payfone's or Affiliate's business.

A Severity 3 Error causes a minor function of the facilities and/or software to be unavailable or impaired, which adversely affects or is likely to adversely affect, Payfone's or Affiliate's business.

A Severity 4 Error causes a minor function of the facilities and/or software to be impaired, but there is no likely adverse effect on Payfone's or Affiliate's business.

Notwithstanding the availability of a Work-Around, TRUSTID will continue to work to fix the Error and, in any event, provide Payfone with the applicable permanent correction within: (i) ten calendar days for a Severity 1 or 2 Error; or (ii) three weeks for a Severity 3 or 4 Error.

As used herein, a "Work-Around" means a temporary work-around, patch or bypass supplied by TRUSTID in order to temporarily correct an Error; provided that: (i) the facilities' and/or software's functionality, compatibility or use is not adversely affected; and (ii) the Work-Around is not unduly burdensome to Payfone.

2. Notification of Errors; Response. Payfone notifies TRUSTID of Errors and the Severity Levels of such Errors, via TRUSTID's Network Operations Centers (NOC) at (888) 300-3776 and/or via e-mail at support@trustid.com. TRUSTID will respond to Payfone by phone or email as soon as possible and in any event within the relevant response time set forth in Section 1 of this Exhibit C.

3. Error Resolution. If Payfone notifies TRUSTID of a Severity 1, 2 or 3 Error, TRUSTID will assign a technical resource to correct such Error within the relevant response time for such Error. The technical resource will use best efforts to correct the Error in an expeditious manner and will inform Payfone of the technical resource's progress, including the steps taken to resolve the Error, the expected time for resolution of the Error and any resolution of the Error.

4. Error Escalation. If the Error has not been corrected, or a Work-Around has not been provided, within the relevant correction time periods set forth in Section 1 of this Exhibit C, then TRUSTID will escalate the Error immediately to TRUSTID's senior technical resource for managing the facilities. The senior technical resource will use best efforts to correct the Error in an expeditious manner and will inform Payfone of the senior technical resource's progress, including the steps taken to resolve the Error, the expected time for resolution of the Error and any resolution of the Error. TRUSTID will provide the senior technical resource with as much assistance as necessary to fix the problem as soon as possible.

5. TRUSTID will provide Payfone with prior written notice (by as much time as practicable but in no event less than seven calendar days) of the release by TRUSTID of any Upgrade and, except as set forth below, will install and incorporate such Upgrade as part of the applicable Services, at no additional cost. If Payfone requests TRUSTID to demonstrate such Upgrade, TRUSTID will promptly demonstrate such Upgrade to Payfone at no additional cost. If any Upgrade is installed, such Upgrade will thereupon be deemed to be part of the Services.

EXHIBIT D

Service Level Agreement – Service Credits and Root Cause Analyses

1. Overview

TRUSTID understands the importance of the Services' availability and performance and the impact that both have on our customers' operations. To ensure service availability, TRUSTID provides geographically diverse service locations for both primary and backup servers. TRUSTID's service is designed to achieve very high levels of availability.

2. Definitions

Scheduled Maintenance – An activity that has planned service downtime and is scheduled in advance during the weekly Scheduled Maintenance Window.

Written notice shall be provided to the Payfone at least seven calendar days prior to the Scheduled Maintenance activity. Such notice shall include a summary description of the work to be completed and an estimated timeframe of the planned activity.

When needed, TRUSTID's Scheduled Maintenance window is typically Tuesdays from 9:30 p.m. PST until 12:30 a.m. PST the following morning.

TRUSTID will record the details of any Scheduled Maintenance, including the start and end time rounded to the nearest minute, in a Scheduled Maintenance log.

Outage – The Service is not available in accordance with the Agreement for more than three consecutive minutes and it is not due to Scheduled Maintenance. If at least one of the Service endpoints that TRUSTID has made available to Payfone is operational, no Outage has occurred.

For each Outage, TRUSTID shall notify the Payfone by email within thirty minutes of becoming aware of an Outage or as soon thereafter as practicable. TRUSTID shall determine (acting reasonably) when the Outage occurred and record details about it, including the start and end time rounded to the nearest minute, in an Outage log. TRUSTID shall email copies of logs to Payfone upon request.

Outages do not include the failures of Payfone systems or networks, failures of the Internet at large (but without prejudice to TRUSTID's hosting obligations and requirement to have diversely routed connectivity to the Internet) or the inability of Payfone's Internet access provider(s) to route Payfone traffic successfully across the Internet to TRUSTID's Service.

3. Response Time

This measures the elapsed time between TRUSTID's receipt of an API request and TRUSTID's transmission of the response to the request by the Service. Response Time does not include any time required by a Payfone system to send, to receive or to process the request, or any Internet latency. Response Time shall be computed and reported as a monthly average of all Payfone requests received by the Service.

Service Credits

In any month where the average monthly Response Time exceeds nine seconds, a Performance Payment of three percent of that month's transaction fees shall be credited to the Payfone.

4. Availability

This measures the percentage of time within a calendar month that the Service did not experience an Outage, as defined in the Section entitled "Definitions." Availability shall be computed and reported as the monthly percentage obtained from the following formula:

Availability % = (TM – SMM – OM) / (TM – SMM)

where:

TM = Total Minutes in the calendar month
SMM = Scheduled Maintenance Minutes in the calendar month within the agreed maintenance window
OM = Outage Minutes in the calendar month

Service Credits

In any calendar month where Availability falls below 99.6%, a service credit of two percent of that month's processing fees shall be credited to Payfone.

In any calendar month where Availability falls below 99.1%, a service credit of five of that month's processing fees shall be credited to Payfone.

In any calendar month where Availability falls below 98%, a service credit of ten percent of that month's processing fees shall be credited to Payfone.

5. Root Cause Analysis

Where an Outage occurs or a service credit accrues, TRUSTID shall undertake a root cause analysis of the problem and shall take all steps reasonably open to it to investigate, identify and fix the cause. TRUSTID will provide Payfone with updates on the progress of each Root Cause Analysis.

6. Review and Change

Payfone may review service levels with TRUSTID on a mutually agreed date.

EXHIBIT E

Compliance with Data Protection Laws and Regulations

For the purpose of this Exhibit E, personal data means information relating to Payfone's customers and/or employees that Payfone has a legal duty to protect under one or more applicable data protection laws.

A. General Undertakings with Respect to Personal Data

TRUSTID represents, warrants and covenants that:

- it will process, use, maintain and disclose personal data only as necessary for the specific purpose for which this information was disclosed to it and only in accordance with the express instructions of Customer (e.g. to perform services) and for other purposes expressly permitted in this Agreement;
- it will not disclose any personal data to any third party (including, without limitation, to the subject of such information) or any person who does not have a need to know such personal information;
- it will immediately notify Customer in writing if it becomes aware of any disclosure or use of any personal information in breach of this Exhibit E;
- it will cooperate with Customer and the relevant supervisory authority in the event of litigation or a regulatory inquiry concerning the information and shall comply with all lawful and reasonable instructions of Customer and the relevant supervisory authority with regard to the processing of such personal information;
- it will enter into further agreements as reasonably requested by Customer to comply with laws and regulations from time to time; and
- it has no reason to believe that any applicable law will prevent it from fulfilling its obligations under this Exhibit E.

For compliance with US privacy and data protection:

TRUSTID represents, warrants and covenants that it will implement and maintain an appropriate written information security program, the terms of which shall meet or exceed the requirements for financial institutions under 17 CFR 248.30, and which shall include appropriate technical and organizational measures to: (i) ensure the security and confidentiality of all information provided to it by Customer, including, without limitation, personal information (collectively, the "information"); (ii) protect against any threats or hazards to the security or integrity of information, including, without limitation, unlawful destruction or accidental loss, alteration and any other form of unlawful processing; and (iii) prevent such unauthorized access to, use or disclosure of the information;

For compliance with non-US Data Protection Regulations:

In the event that the Services are subject to regulation under the laws of any jurisdiction outside of the United States of America, the parties shall execute such further documents and shall take such further actions as may be required to ensure and to demonstrate compliance with all applicable such regulations.

B. **Undertakings Related to Customer Incoming Numbers**.

1. **Background**

TRUSTID will receive telephone numbers in the course of providing Services to Customer or its Affiliates that purport to be the number from which a caller is calling Customer ("Customer Incoming Numbers") to improve operations. The fact that a call was made or purported to have been made from a Customer Incoming Number is Confidential Information.

2. **Scope of usage**

Subject to paragraph 3 below, but otherwise notwithstanding any other provision of this Agreement, as part of its Services, TRUSTID may, both during and after the Term of this Agreement, use the Customer Incoming Numbers:

(a) as required for providing the Services to Customer under this Agreement;
(b) for calculating and verifying invoices to Customer under this Agreement;
(c) for audit (including external audit where external auditors are subject to confidentiality obligations); and
(d) for performing internal technical analysis on the ANI relating to the Customer Incoming Numbers to verify or improve TRUSTID's technology.

3. **Prohibited usage**

Except in connection with activities specifically permitted in Section 2 TRUSTID will not:

- Disclose any Customer Incoming Number to any third party
- Use any Customer Incoming Number to send or make any communication to or with an individual or to make a phone call or send a voice message or text message to any Customer Incoming Number;
- Use any Customer Incoming Number to perform any identification of individuals or to find out, estimate, surmise or establish any information relating to any individual or groups of individuals;
- Use, link or associate any Customer Incoming Number with any other personal information.

EXHIBIT F

Insurance

At all times during the Term of this Agreement, TRUSTID will maintain in force with reputable insurance carriers the following insurance:

$2,000,000	General Liability
$4,000,000	Annual Aggregate
$312,120	Business Personal Property - Blanket Limit - $500 Deductible
Included	Business Income/Extra Expense
$1,000,000	Crime Package including Employee Dishonesty & ERISA
$5,000,000	Technology Errors & Omissions Liability/Each Occurrence and Aggregate
$1,000,000	Sublimit for Privacy Regulation Proceeding - $10,000 deductible
$1,000,000	Sublimit for Privacy Event Expense - $10,000 Deductible
$1,000,000	Sublimit for Network Extortion - $10,000 Deductible
$1,000,000	Hired Auto Liability
$1,000,000	Non owned Auto Liability
$4,000,000	Umbrella Liability
$3,000,000	Directors & Officers Liability - $10,000 Self-Insured Retention
$1,000,000	Fiduciary Liability - $0 Self-Insured Retention
$1,000,000	Employment Practice Liability - $10,000 Self-Insured Retention
$500,000	Employers Liability
Statutory	Workers Compensation

Exhibit 17

A toolkit to enable Trust, Visibility and Control.

Boost customer satisfaction and retention by enabling incredible digital experiences with our award-winning modular Trust Platform.

Request a Meeting

Trust Matters.

Experts predict that Trust will reshuffle the Fortune 500. Why? Trust allows companies to enable the exceptionally easy and secure digital experiences that today's customers crave and expect. This means happier customers and better retention.

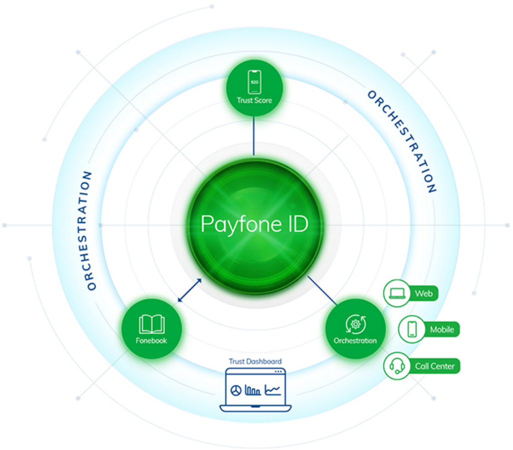
Greater Digital Experiences

Trusted Customers

Higher Customer Satisfaction

Trust Platform

Payfone's patented Trust Platform is modular and is built around the Trust Score, tokenized Payfone ID, Fonebook, Orchestration and the Payfone Dashboard.



Fonebook

Fonebook's next-generation identity tokenization technology delivers better security, easier digital experiences and faster response across all channels.

With your customized company Fonebook, you can verify and append your customer information for more robust and accurate data to confidently and more effectively engage with your customers.

Payfone ID

Through your Fonebook, a unique Payfone ID is generated for every customer. This secure ID token becomes their universal identifier to facilitate and unlock enhanced digital experiences.

Our patented tokenization technology replaces sensitive personal information with a token that is virtually meaningless to anyone other than the entity that created it.

Tokenization delivers better security, easier digital experiences, and faster response across all customer channels.

Payfone's secure ID tokens eliminate cumbersome fraud processes, which diminish the customer experience and negatively impac

Trust Score

The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.)

In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust.

The Trust Score lets businesses confidently service customers and promote new offers.

Instead of relying on static, hackable methods such as passwords, security questions and SMS passcodes...

The Payfone Trust Score analyzes real-time digital signals from a multitude of sources.

980

To generate a dynamic score that answers the question "Can this customer be trusted?"

Payfone's recommended thresholds:

0-300

Decline recommended

300-640

Further inspection recommended

≥640

Approve with no friction

https://www.payfone.com/trust-platform/ Go

JUL NOV DEC

08

2018 2019 2020

3 captures

3 Jun 2019 - 8 Nov 2019

About this capture

https://www.payfone.com/trust-platform/ Go

JUL NOV DEC
08
2018 2019 2020

3 captures
3 Jun 2019 - 8 Nov 2019

About this capture

https://www.payfone.com/trust-platform/ Go JUL NOV DEC 08 2018 2019 2020

3 captures
3 Jun 2019 - 8 Nov 2019

About this capture

Let us help you reach your goals with an innovative Trust Platform that enables you to extend faster, frictionless and fraud-free experiences to all of your customers.

Request a Meeting

PAYFONE

Home
Trust Platform
Products

Company
Resources
Press and News

Contact Us
Careers Now Hiring

Privacy Policy Exercise Your Rights Do Not Sell My Personal Information

Exhibit 18

CASE STUDY

Prove Empowers Fortune 200 Retailer's Call Center Agents to Reduce Fraud and Maximize Revenues

By the Numbers

98%

Success Rate

Prove achieved an outstanding uplift in their success rate (Ap**prove** Rate), from 83% in 2018 to **98% with Prove in 2019.**

50

Seconds Reduced

Prove helped the company significantly reduce their call times by 50 seconds, from 600 in 2018 down to **550 seconds in 2019**.

52%

Decreased Fraud Rate

Prove contributed to a substantial **52% decrease in the company's fraud rates.**

About the Company

With over 1,000 locations in most of the fifty states, this company is one of the largest family-oriented department store retail chains in the US. They offer clothing, footwear and accessories, as well as home products and housewares targeted to middle income customers. They recently reported revenues of approximately $20B and net income of just under $1B.

Executive Summary

Looking to decrease fraud and reduce call center handling times while demonstrating a better return on investment than other solutions offered, the company turned to Prove for help.

The Need

Putting customers first and offering them personalized connections and easy experiences are core tenets of the company's strategic values.

These values manifest themselves in the way the company structures and operates their call centers: unlike many organizations in the industry that have moved to reduce the number of call center agents in favor of automated interactive voice response (IVR) models, this company aims to keep their call center agents engaged and to empower them to provide human-centered concierge service to their customers.

The company's call center performs a key role in stepping up authentication for suspicious orders coming from across all channels. Agents need to balance out vigilance to prevent fraudulent transactions

1,800

# of Agents Using Trust Portal Today

Prove originally piloted Trust Portal with 30 call center agents across two teams. Today, there are **1,800 agents using Trust Portal across 12 sites.**

with providing a seamless consumer experience. In order to accomplish these goals, they need to be equipped with the right tools.

The Solution

The company's call center's fraud department adopted Prove's Trust Portal solution. Trust Portal is designed to help agents, in real time, expedite manual reviews to assess risk more rapidly to better service consumers and prevent fraud. It eliminates their dependency on IT and developer teams and allows them to directly access Prove's capabilities with an intuitive, GUI-based experience. The SaaS-based, full-featured Trust Portal requires no integration, and with fast provisioning and immediate access, accelerates the organization's time to value.

With Trust Portal, the company's agents can:

- Verify that a caller's phone number matches their address for order delivery (Prove Identity Verification)
- Measure the risk and reliability of the caller's phone number to confirm that it has not been compromised (Prove Trust Score)
- Validate that the caller is in possession of the phone making the call (Prove Instant Link for Web (Fortified OTP) or Voice OTP)

Using Prove's three-pronged verification and authentication approach allows the agents to expedite handle times while mitigating fraud risk.

The Results

Initial results demonstrated the power of Prove's platform, which helped agents provide a much more seamless and personable experience to their consumers. The company placed Prove at the top of their authentication waterfall and reduced their dependency on other fraud prevention vendors, thereby streamlining their architecture and lowering overall costs.

Based on these initial results and the strong partnership between the two organizations, Prove continued to collaborate with the company to address new fraud vectors. Prove also delivered advanced features, including deeper searching capabilities and integration with their corporate single sign-on platform, further improving the agents' user experience with Trust Portal.

Exhibit 19

The Modern Platform for Continuous Identity Authentication

Prove secures the digital onboarding, servicing, call center and payment services of over 1,000 enterprises and 500 banks including 8 of the top 10 U.S. banks.

Prove’s global cloud solutions and mobile intelligence (https://www.payfone.com/insights/what-is-phone-intelligence/?__hstc=207985293.13ba3bac966b63a06f0333a029c1d6ee.1605577175065.1605577175065.1605577175065.1&__hssc=20
driven APIs significantly increase the Ap**prove** Rates (https://www.payfone.com/insights/did-you-know-3-critical-kpis-to-measure-digital-trust/?__hstc=207985293.13ba3bac966b63a06f0333a029c1d6ee.1605577175065.1605577175065.1605577175065.1&__hssc=20
of digital transactions while mitigating fraud with a focus on accuracy, ease and privacy.

Payfone is now Prove!

Payfone Rebrands to Prove & Raises $100 Million (https://prove.com/blog/prove-sets-standard-for-modern-identity-authentication-with-new-brand-major-acquisition-and-100m-investment-for-global-expansion/) Read More (https://prove.com/blog/prove-sets-standard-for-modern-identity-authentication-with-new-brand-major-acquisition-and-100m-investment-for-global-expansion/)

Prove Sees 300% Increase in YoY New Business Wins, Now Serves 9 of the Top 10 Financial Institutions Read More (https://prove.com/blog/prove-sees-300-increase-in-yoy-new-business/)

The new prove.com website is coming soon

Go to Payfone.com (https://www.payfone.com/?__hstc=207985293.13ba3bac966b63a06f0333a029c1d6ee.1605577175065.1605577175065.1605577175065.1&__hssc=207985293.1.1605577175066&

Securing 1,000+ global enterprises and 500+ banks including 8 of the top 10 in the US

The Identity Verification & Authentication Leader

20 billion
Transactions in 2019

1000+ Enterprise Customers

Privacy-First, Decentralized

Coverage of 95% of
US Adults

195 Global Markets

4 Reasons Top Companies Choose Prove

1. Persistent identity verification that covers 90% of US adults and stays updated through phone number ownership and device lifecycle events
2. Omni-channel, passive authenticators that prove possession over mobile, desktop, call center, and chat
3. Our Trust Score™ delivers federated trust with real-time analysis of the behavior and velocity of billions of phone number and device authentication events, as well as the most robust coverage of modern fraud vectors such as burner phones, SIM swaps, account ports, SPID and line type changes, recycled and reassigned phone numbers, and synthetic identities
4. Privacy-first approach to data emphasizes a decentralized data architecture, identity tokenization, consent, and limits on data aggregation

Award-Winning Technology

(https://www.payfone.com/press/payfone-ranked-in-the-americas-fastest-growing-companies-by-the-financial-times/?__hstc=207985293.13ba3bac966b63a06f0333a029c1d6ee.1605577175065.1605577175065.1605577175065.1&__hssc=207985293.1.1605577175066&__hsfp=3629513924)

(https://www.payfone.com/press/payfone-makes-deloitte-fast-500-list-of-fastest-growing-tech-cos-3rd-year-in-a-row/?__hstc=207985293.13ba3bac966b63a06f0333a029c1d6ee.1605577175065.1605577175065.1605577175065.1&__hssc=207985293.1.1605577175066&__hsfp=3629513924)

(https://www.payfone.com/press/payfone-wins-best-customer-security-and-over-the-top-ott-monetization-awards-in-the-fourth-annual-fierce-innovation-awards-telecom-edition/?__hstc=207985293.13ba3bac966b63a06f0333a029c1d6ee.1605577175065.1605577175065.1605577175065.1&__hssc=207985293.1.1605577175066&__hsfp=3629513924)

(https://www.payfone.com/press/payfone-wins-sinet-16-cybersecurity-innovator-award/?__hstc=207985293.13ba3bac966b63a06f0333a029c1d6ee.1605577175065.1605577175065.1605577175065.1&__hssc=207985293.1.1605577175066&__hsfp=3629513924)

(https://www.payfone.com/press/payfone-announced-as-a-consumer-protection-finalist-in-the-2018-edison-awards/?__hstc=207985293.13ba3bac966b63a06f0333a029c1d6ee.1605577175065.1605577175065.1605577175065.1&__hssc=207985293.1.1605577175066&__hsfp=3629513924)

Privacy Policy (https://www.payfone.com/privacy-policy/?__hstc=207985293.13ba3bac966b63a06f0333a029c1d6ee.1605577175065.1605577175065.1605577175065.1&__hssc=207985293.1.1605577175066&__hsfp=3629513924)

Exercise Your Rights (https://www.payfone.com/exercise-your-rights/?__hstc=207985293.13ba3bac966b63a06f0333a029c1d6ee.1605577175065.1605577175065.1605577175065.1&__hssc=207985293.1.1605577175066&__hsfp=3629513924)

Do Not Sell My Personal Information (https://privacyportal-cdn.onetrust.com/dsarwebform/8aa1d8bb-97e7-4099-80ca-30899517246c/01791f6c-c9d7-49c8-a2ed-91155f5a1279.html)

Exhibit 20

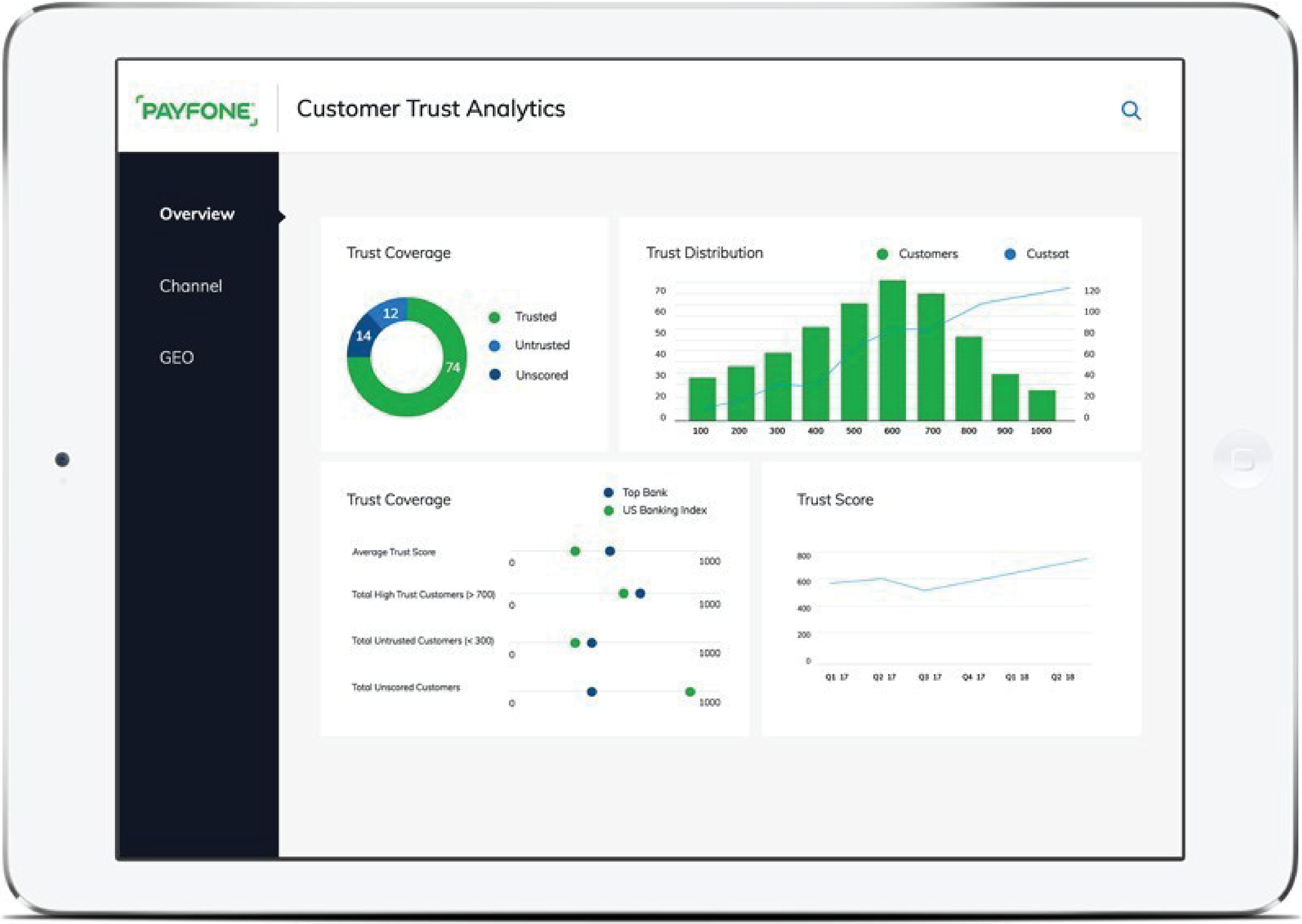

PAYFONE
Customer Trust Analytics
Overview
Channel
GEO
Trust Coverage
12
14
74
Trusted
Untrusted
Unscored
Trust Distribution
Customers
Custsat
70
60
50
40
30
20
0
120
100
80
60
40
20
0
100
200
300
400
500
600
700
800
900
1000
Trust Coverage
Top Bank
US Banking Index
Average Trust Score
Total High Trust Customers (> 700)
Total Untrusted Customers (< 300)
Total Unscored Customers
0
1000
Trust Score
800
600
400
200
0
Q1 17
Q2 17
Q3 17
Q4 17
Q1 18
Q2 18

Exhibit 21

https://www.payfone.com/ Go JAN FEB MAR
362 captures ◀ 06 ▶
12 Dec 1998 - 18 Jun 2020 2016 2017 2018
About this capture

Instant Trust

Removes friction, drives engagement and fights fraud with the power of instant mobile authentication

OUR SOLUTIONS

Enrollment

Integrate new people, numbers and devices with speed, without friction

OTP Replacement

Authenticate every mobile login without complications

Call Verification

Instantly verify incoming calls into your contact center

Fortified OTP

Protect SMS verification messaging from evolving threats

ABOUT PAYFONE

In today's business world, a few bad actors can force businesses to treat all customers with suspicion. This leads to client and employee frustration, higher operating costs and lower revenue.

Payfone delivers seamless, non-intrusive verification using each mobile phone's inherent identity to provide top-tier protection for businesses and their customers.

Remove friction and drive user engagement with Payfone Instant Trust. It's the best way to enhance the customer experience while lowering the risk friction and fraud.

SOLUTIONS	COMPANY	SUPPORT	LOCATIONS
Enrollment	Investors	Contact	New York Office

Fortified OTP

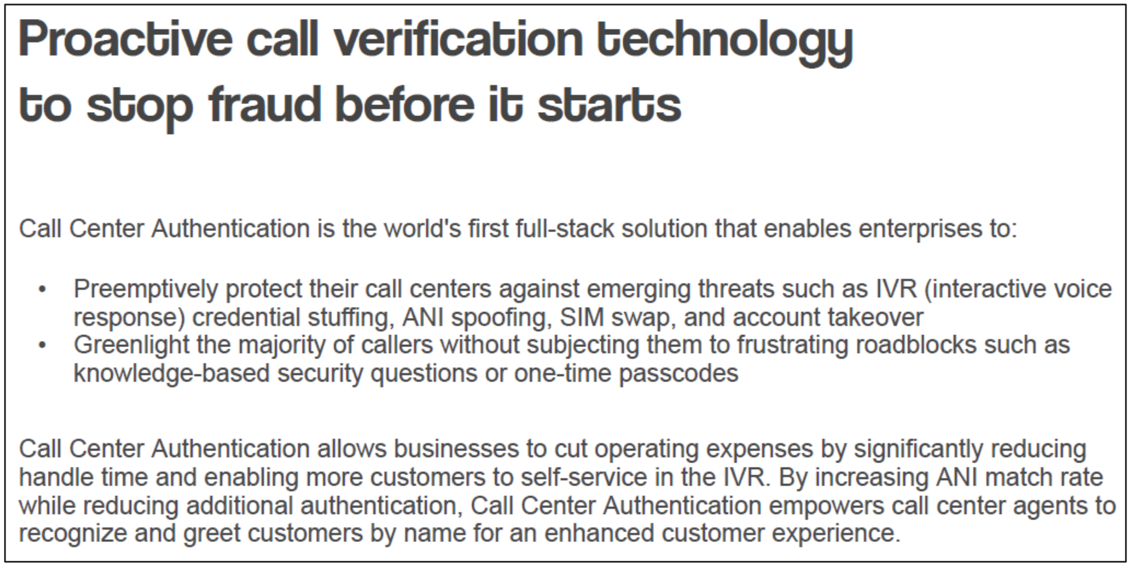
Denver Office
6455 S. Yosemite St., Suite 730
Greenwood Village, CO 80111

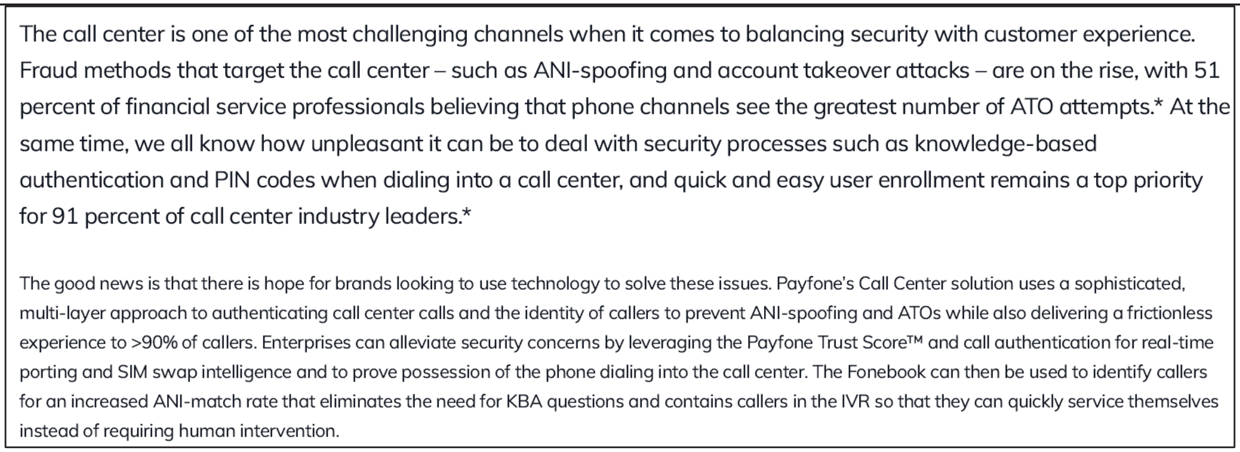
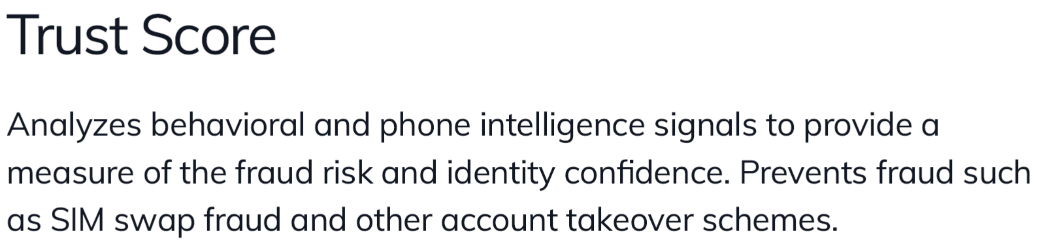
Exhibit 22

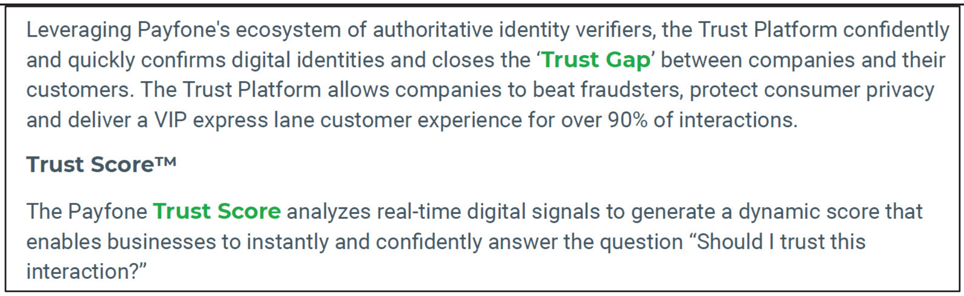
PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT

US 9,001,985 Claim 1

Prove's Call Center Authentication

1. A method of determining a source origin confidence metric of a calling party number or billing number associated with an incoming call to a called party telephonic device from a calling party telephonic device, comprising:	Prove's Call Center Authentication includes a method of determining a Trust Score ("*source origin confidence metric*") of a calling party number associated with an incoming call to a called party telephonic device (e.g., call center) from a calling party telephonic device.  **Proactive call verification technology to stop fraud before it starts** Call Center Authentication is the world's first full-stack solution that enables enterprises to: • Preemptively protect their call centers against emerging threats such as IVR (interactive voice response) credential stuffing, ANI spoofing, SIM swap, and account takeover • Greenlight the majority of callers without subjecting them to frustrating roadblocks such as knowledge-based security questions or one-time passcodes Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience. *Exhibit 9 at 2.*

	 The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.* The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention. *Exhibit 10 at 1.*  Trust Score Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes. *Exhibit 8 at 1-2.*

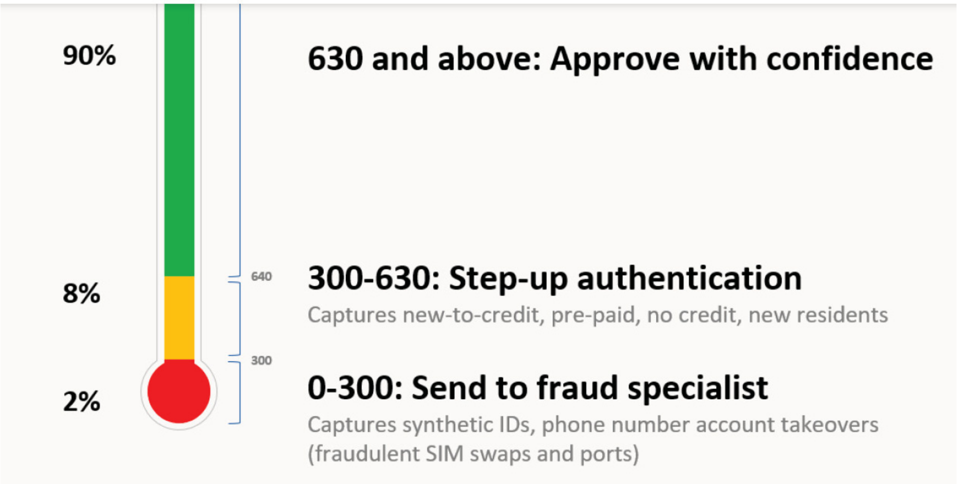


Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the '**Trust Gap**' between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions.

Trust Score™

The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question "Should I trust this interaction?"

Exhibit 11 at 4.



630 and above: Approve with confidence

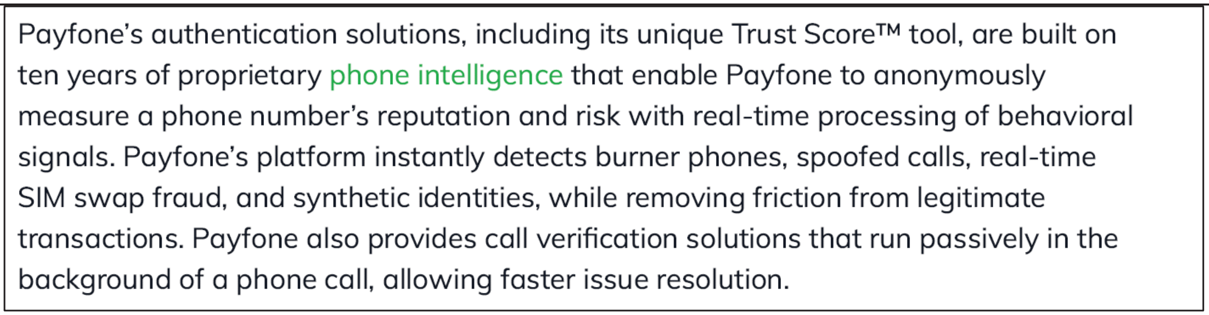
300-630: Step-up authentication

Captures new-to-credit, pre-paid, no credit, new residents

0-300: Send to fraud specialist

Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports)

Exhibit 11 at 5.

	 Payfone's authentication solutions, including its unique Trust Score™ tool, are built on ten years of proprietary phone intelligence that enable Payfone to anonymously measure a phone number's reputation and risk with real-time processing of behavioral signals. Payfone's platform instantly detects burner phones, spoofed calls, real-time SIM swap fraud, and synthetic identities, while removing friction from legitimate transactions. Payfone also provides call verification solutions that run passively in the background of a phone call, allowing faster issue resolution. *Exhibit 15 at 2.*

PRIVILEGED AND CONFIDENTIAL / ATTORNEY CLIENT WORK PRODUCT

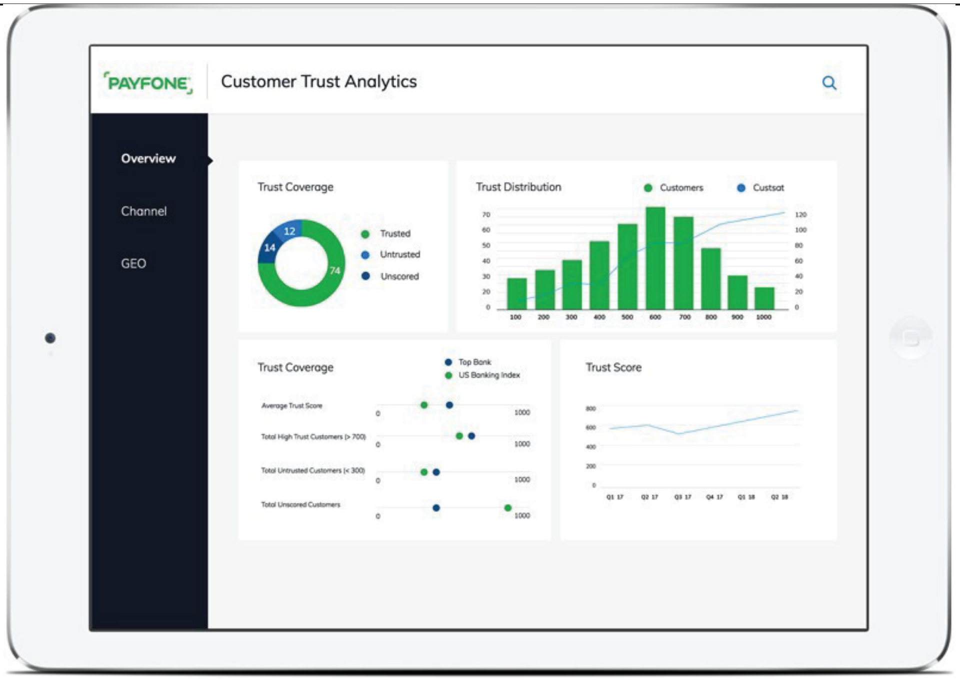
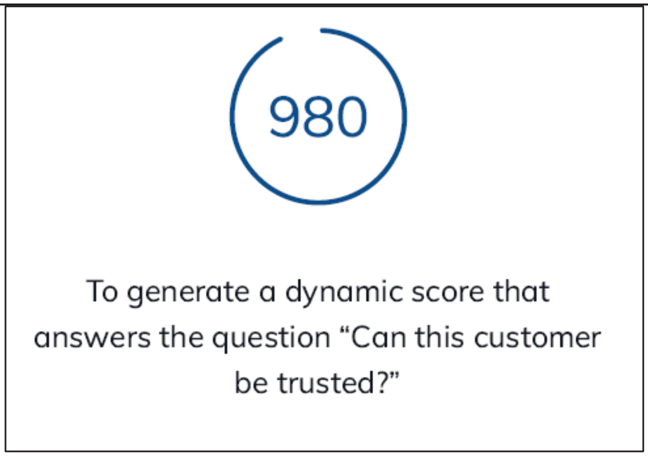
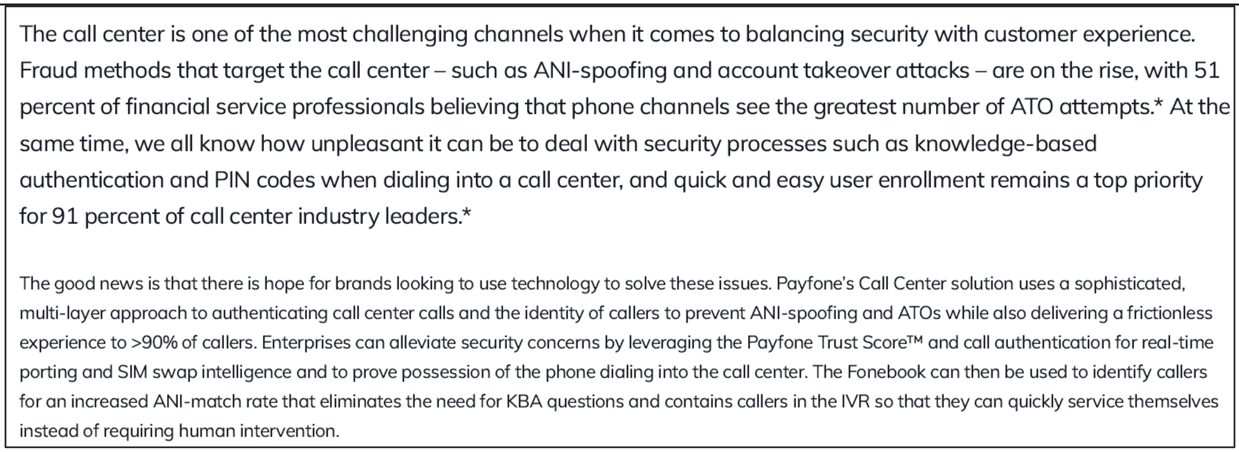
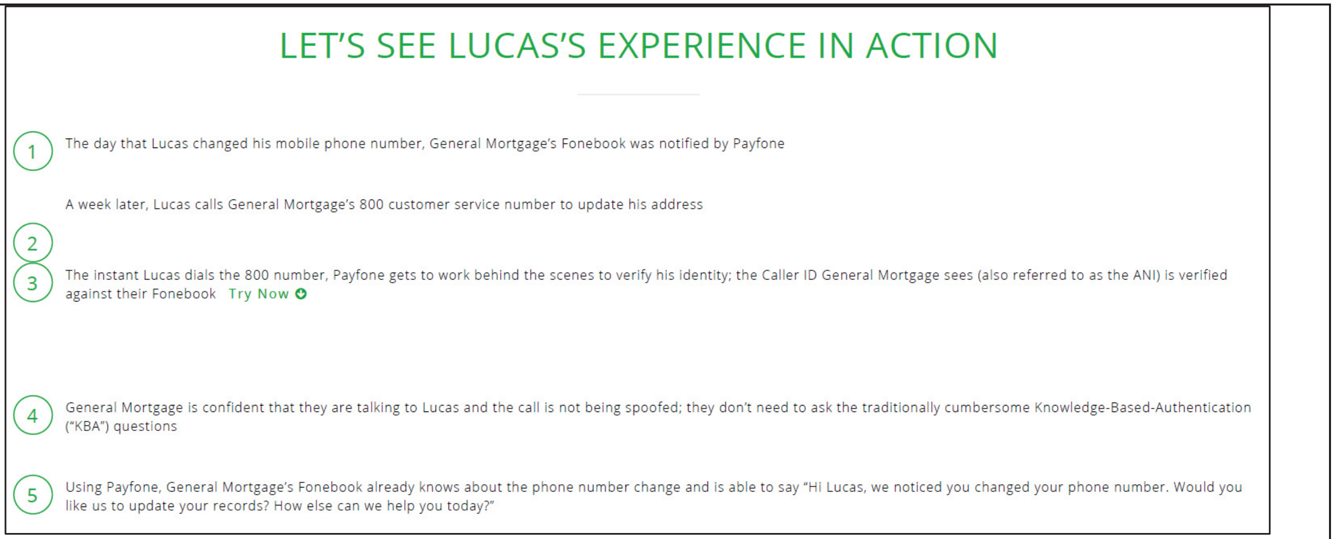
<table>
<tr>
<td></td>
<td>


Exhibit 20 at 1.
</td>
</tr>
</table>

	 To generate a dynamic score that answers the question “Can this customer be trusted?” *Exhibit 17 at 3.*
receiving by an electronic system associated with the called party telephonic device the calling party number or billing number, wherein the electronic system receives the calling party number or billing number from the called party telephonic device;	Prove’s Call Center Authentication is associated with the called party telephonic device (e.g., call center) receives “*the calling party number*” (e.g., ANI) from the called party telephonic device (e.g., call center).

	 The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.* The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention. *Exhibit 10 at 1.*



LET'S SEE LUCAS'S EXPERIENCE IN ACTION

1 The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone

2 A week later, Lucas calls General Mortgage's 800 customer service number to update his address

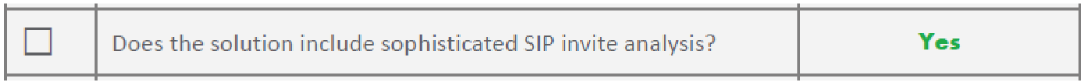
3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now

4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions

5 Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?"

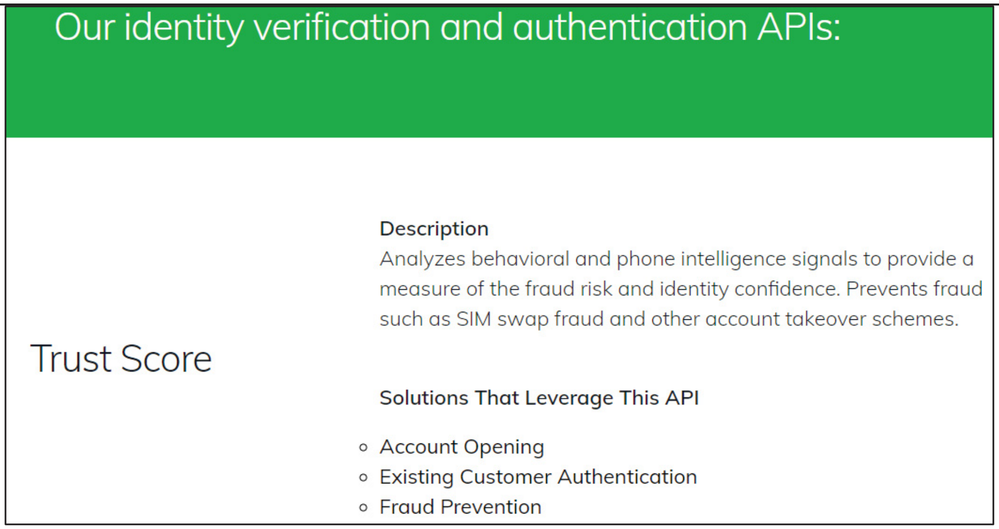
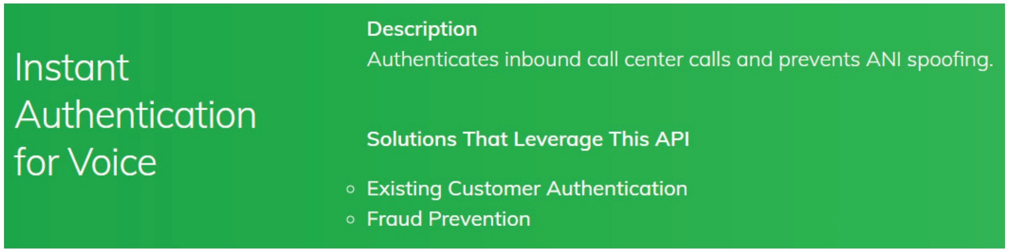
Exhibit 13 at 1.

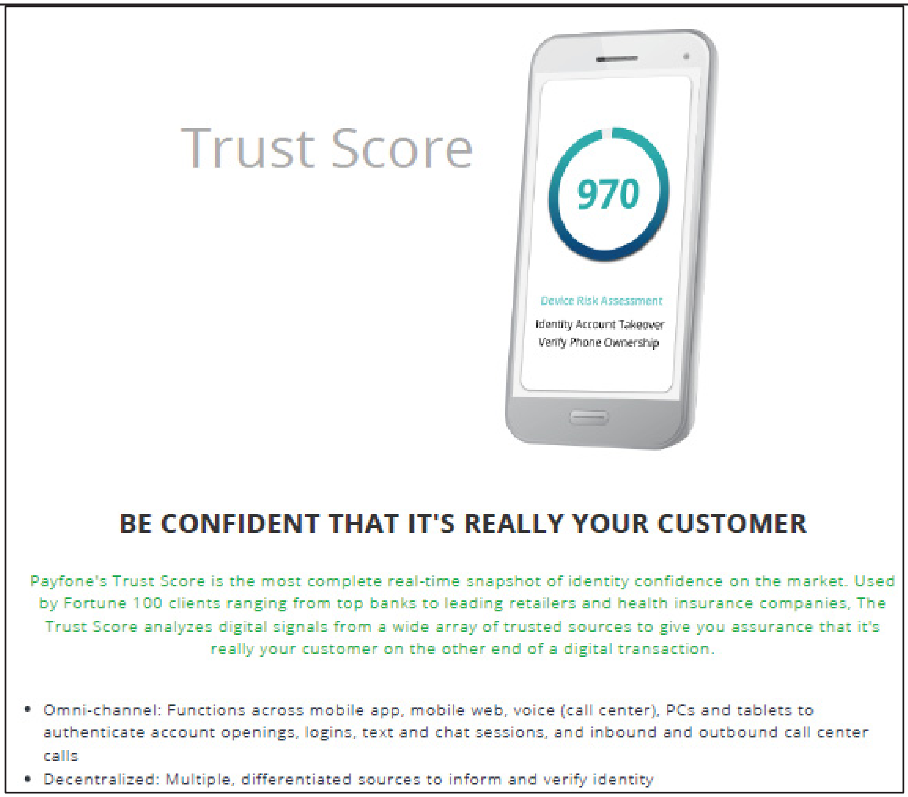
On information and belief, Prove Call Center Authentication receives SIP invite information, including the ANI, from the call center via Prove's APIs.



□	Does the solution include sophisticated SIP invite analysis?	Yes

Exhibit 12 at 1.

	 Our identity verification and authentication APIs: Trust Score Description Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes. Solutions That Leverage This API ○ Account Opening ○ Existing Customer Authentication ○ Fraud Prevention *Exhibit 8 at 2.*  Instant Authentication for Voice Description Authenticates inbound call center calls and prevents ANI spoofing. Solutions That Leverage This API ○ Existing Customer Authentication ○ Fraud Prevention *Exhibit 8 at 4.*

	 Trust Score 970 Device Risk Assessment Identity Account Takeover Verify Phone Ownership **BE CONFIDENT THAT IT'S REALLY YOUR CUSTOMER** Payfone's Trust Score is the most complete real-time snapshot of identity confidence on the market. Used by Fortune 100 clients ranging from top banks to leading retailers and health insurance companies, The Trust Score analyzes digital signals from a wide array of trusted sources to give you assurance that it's really your customer on the other end of a digital transaction. • Omni-channel: Functions across mobile app, mobile web, voice (call center), PCs and tablets to authenticate account openings, logins, text and chat sessions, and inbound and outbound call center calls • Decentralized: Multiple, differentiated sources to inform and verify identity *Exhibit 14 at 1.*
after receiving the calling party number or billing number and before the incoming call is answered, gathering by the electronic system associated with the called party telephonic device operational status information associated with the calling party number or billing number, and	After receiving the "*calling party number*," Prove's Call Center Authentication gathers "*operational status information associated with the calling party number*" (*e.g.*, "billions of digital signals from multiple sources," Fonebook).

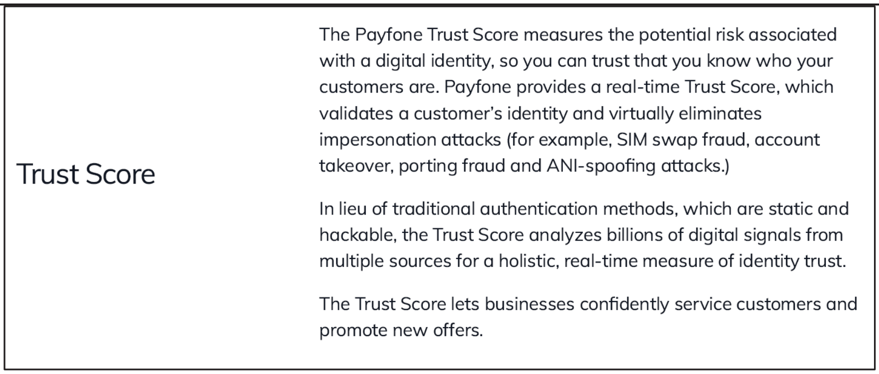
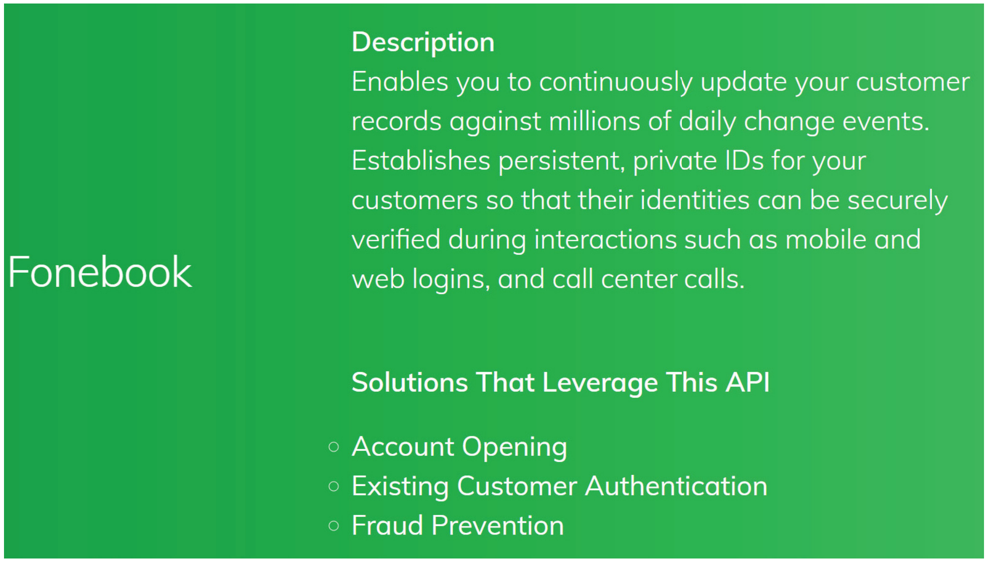
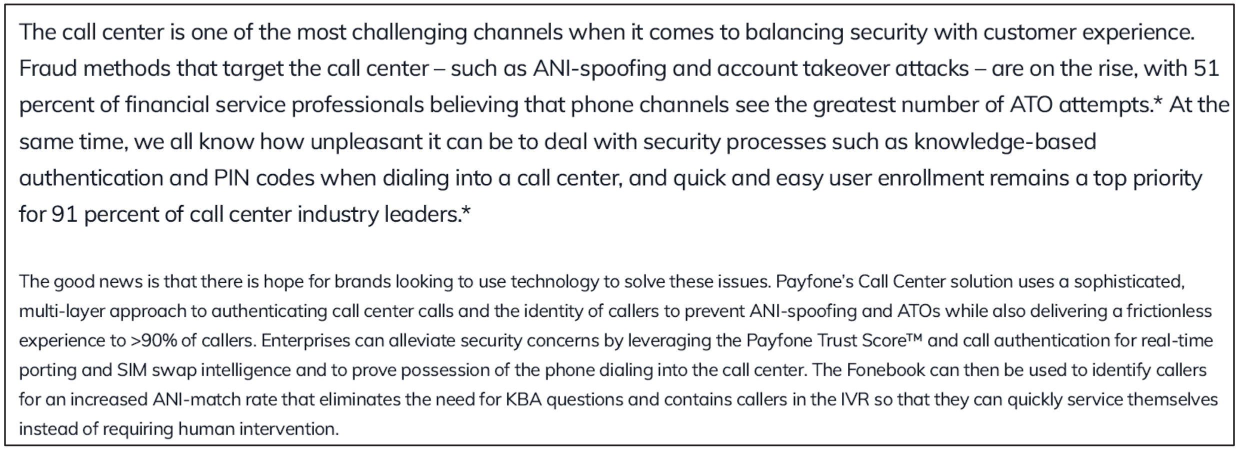
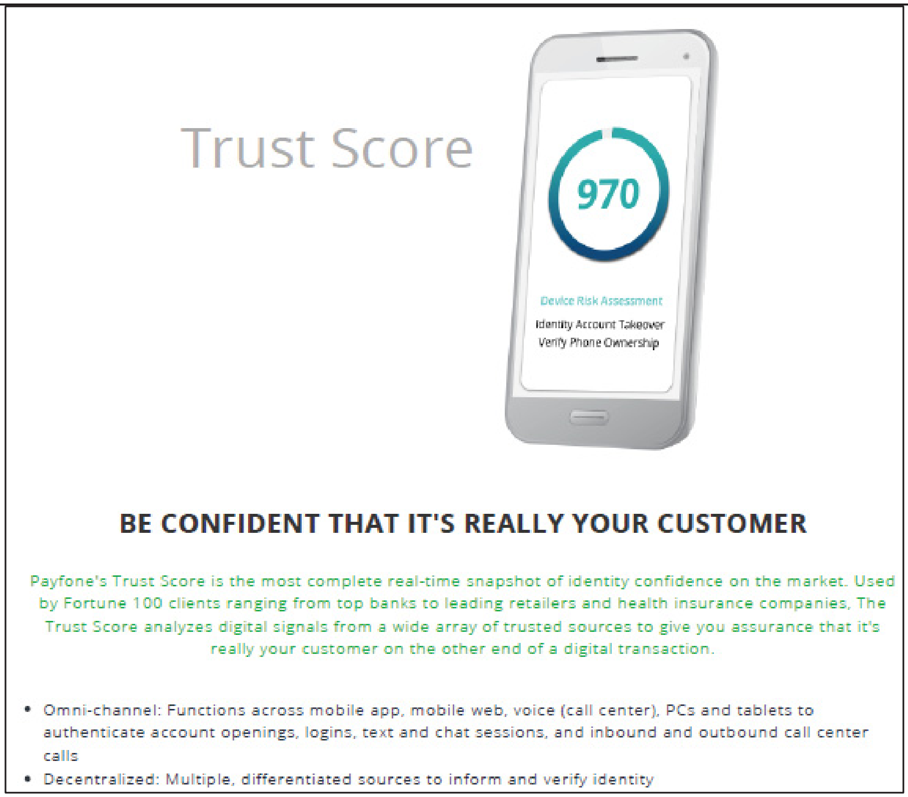
	 Trust Score The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.) In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust. The Trust Score lets businesses confidently service customers and promote new offers. *Exhibit 17 at 3.*  Fonebook **Description** Enables you to continuously update your customer records against millions of daily change events. Establishes persistent, private IDs for your customers so that their identities can be securely verified during interactions such as mobile and web logins, and call center calls. **Solutions That Leverage This API** ○ Account Opening ○ Existing Customer Authentication ○ Fraud Prevention

	Exhibit 8 at 2.  The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.* The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention. *Exhibit 10 at 1.*



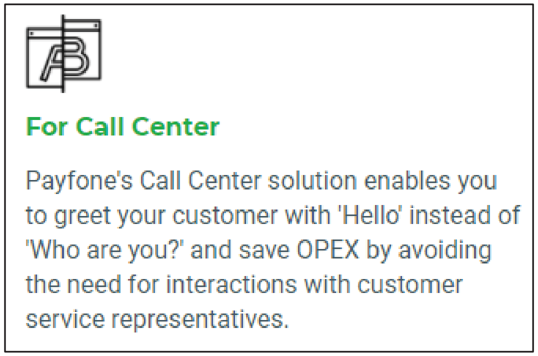
BE CONFIDENT THAT IT'S REALLY YOUR CUSTOMER

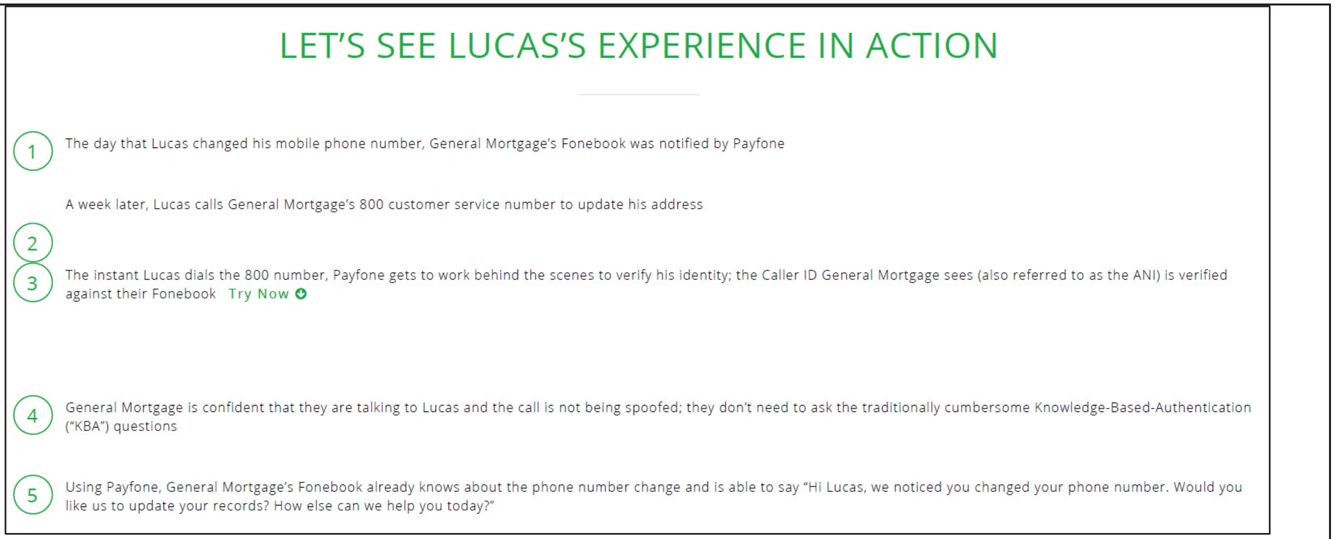
Payfone's Trust Score is the most complete real-time snapshot of identity confidence on the market. Used by Fortune 100 clients ranging from top banks to leading retailers and health insurance companies. The Trust Score analyzes digital signals from a wide array of trusted sources to give you assurance that it's really your customer on the other end of a digital transaction.

- Omni-channel: Functions across mobile app, mobile web, voice (call center), PCs and tablets to authenticate account openings, logins, text and chat sessions, and inbound and outbound call center calls
- Decentralized: Multiple, differentiated sources to inform and verify identity

Exhibit 14 at 1

At a minimum, Rodger Desai indicated that Prove analyzes information such as tenure of a number, behavior, and funding mechanism. *See* Consult Hyperion: Event 21 - Fireside Chat With Rodger Desai, *available at* https://chyp.com/webinars/week-21-fireside-chat-with-rodger-desai/. *See also* Payfone's Rodger Desai: Digital Transactions Should Be As Easy As Making A Phone Call, *available at https://tearsheet.co/podcasts/payfones-rodger-desai-digital-transactions-should-be-as-easy-as-making-a-phone-call/*

	On information and belief, the "*operational status information*" is gathered "*before the incoming call is answered*" because Prove instantly verifies calls.  **For Call Center** Payfone's Call Center solution enables you to greet your customer with 'Hello' instead of 'Who are you?' and save OPEX by avoiding the need for interactions with customer service representatives. *Exhibit 11 at 3.*



LET'S SEE LUCAS'S EXPERIENCE IN ACTION

1 The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone

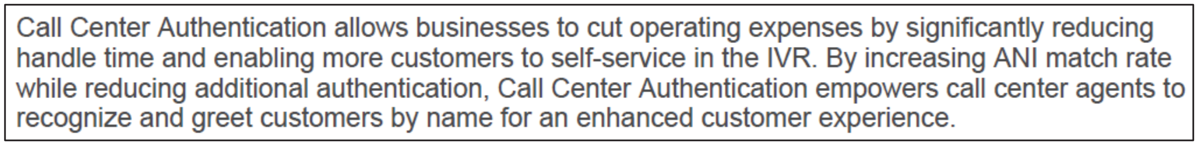
2 A week later, Lucas calls General Mortgage's 800 customer service number to update his address

3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now

4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions

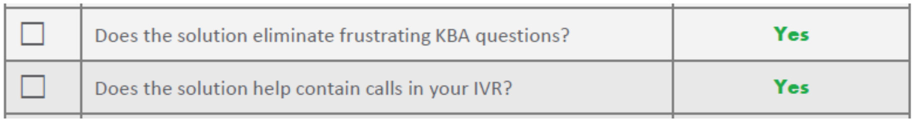
5 Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?"

Exhibit 13 at 1.



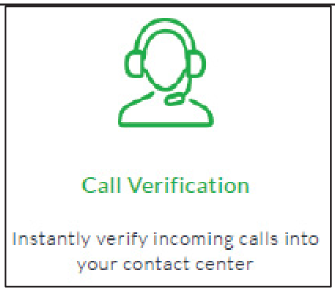
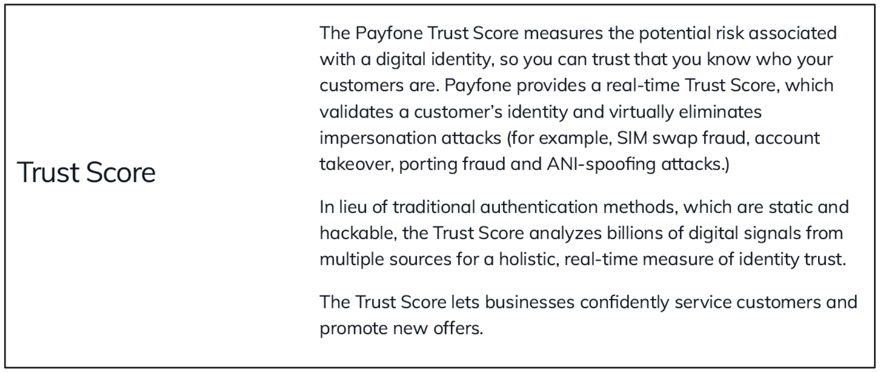
Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience.

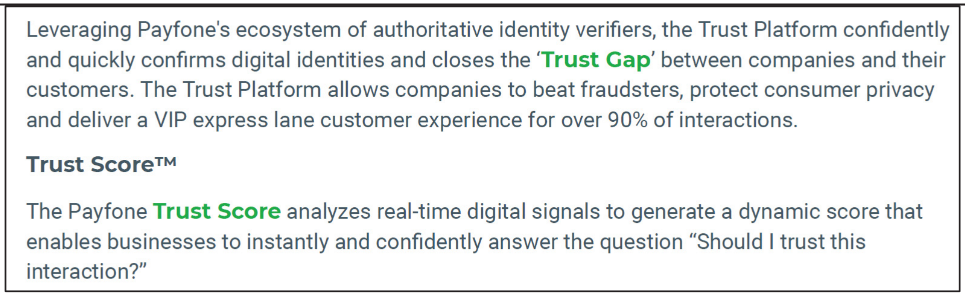
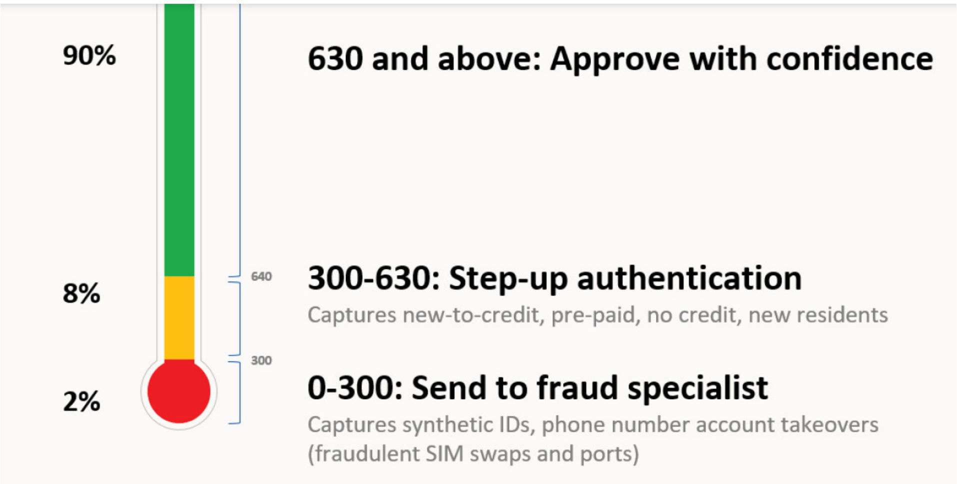
Exhibit 9 at 2.



□	Does the solution eliminate frustrating KBA questions?	Yes
□	Does the solution help contain calls in your IVR?	Yes

Exhibit 12 at 1.

	 Call Verification Instantly verify incoming calls into your contact center *Exhibit 21 at 1.*
determining by the electronic system associated with the called party telephonic device the source origin confidence metric for the calling party number or billing number.	Prove's Call Center Authentication determines a numeric Trust Score (i.e., "*source origin confidence metric*") for the calling party number.  Trust Score The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.) In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust. The Trust Score lets businesses confidently service customers and promote new offers. *Exhibit 17 at 3.*

	 Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the '**Trust Gap**' between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions. **Trust Score™** The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question "Should I trust this interaction?" *Exhibit 11 at 4.*  **630 and above: Approve with confidence** **300-630: Step-up authentication** Captures new-to-credit, pre-paid, no credit, new residents **0-300: Send to fraud specialist** Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports) *Exhibit 11 at 5.*

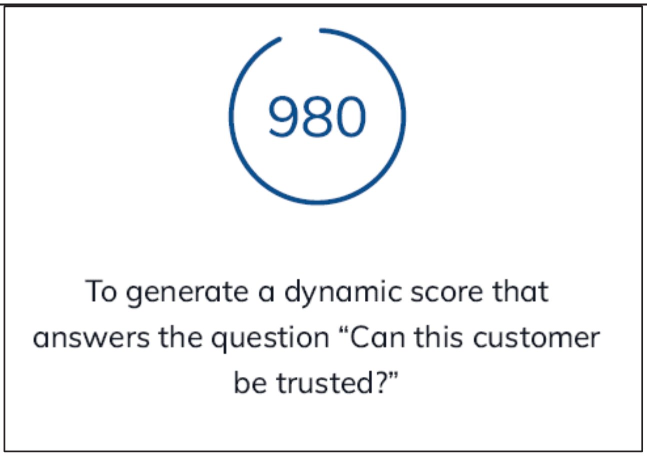
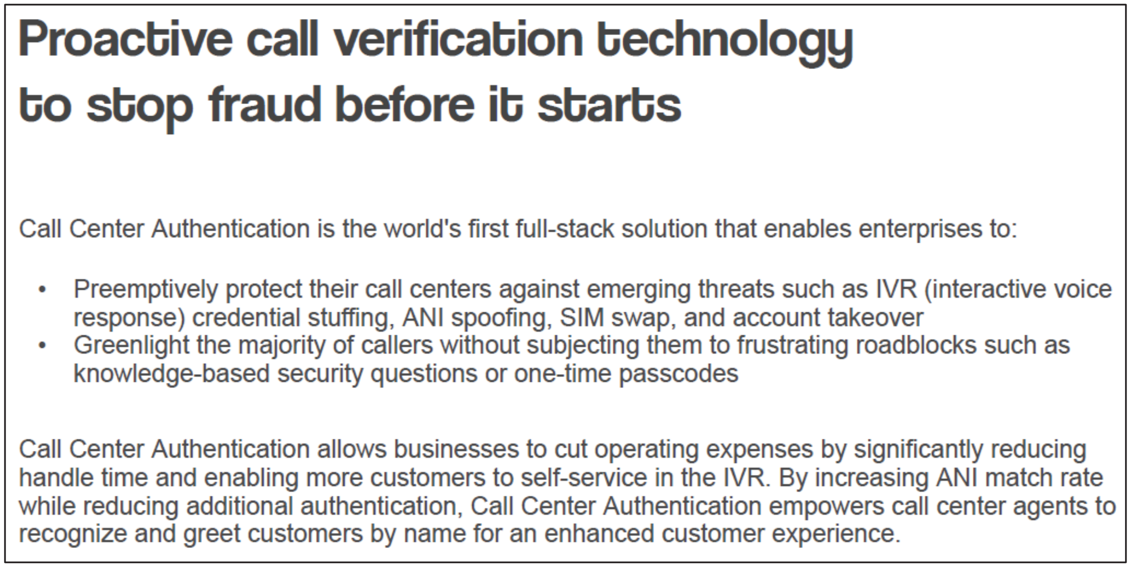
	 To generate a dynamic score that answers the question "Can this customer be trusted?" *Exhibit 17 at 3.*

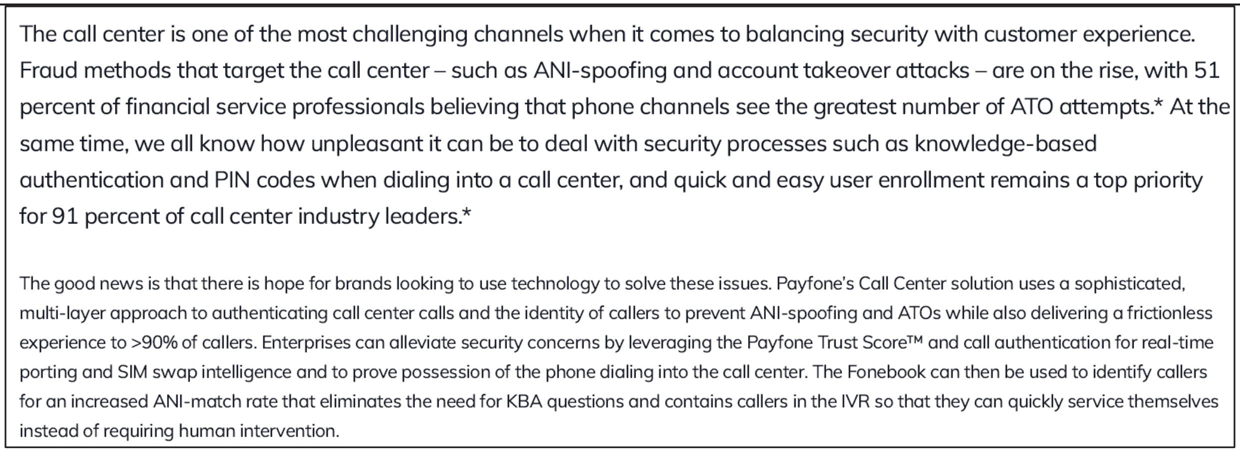
Exhibit 23

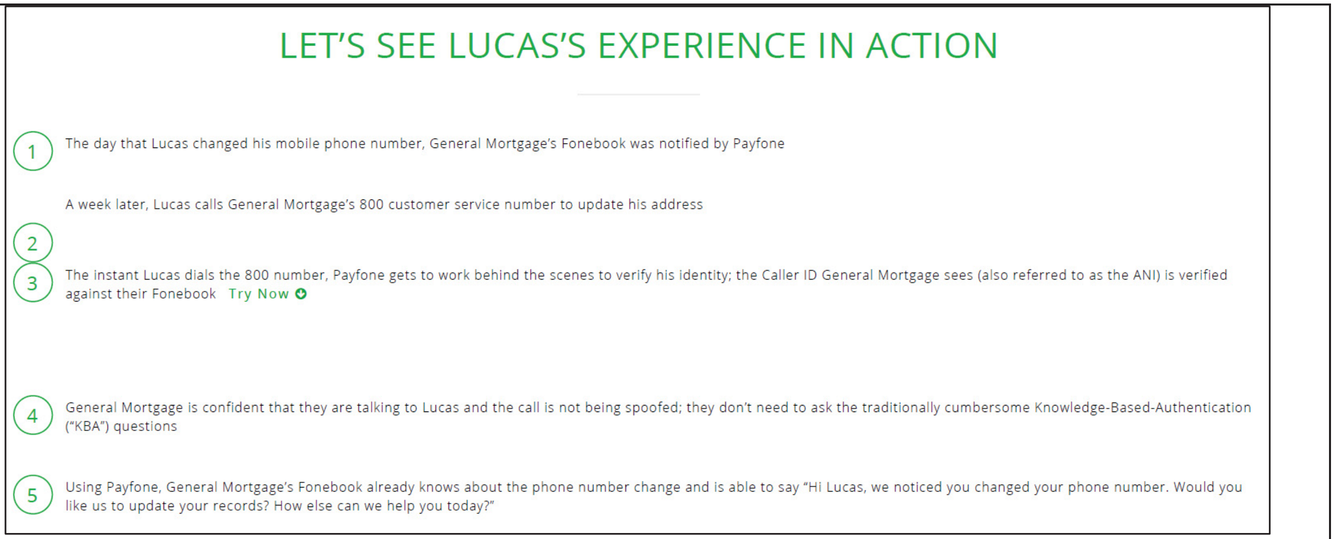
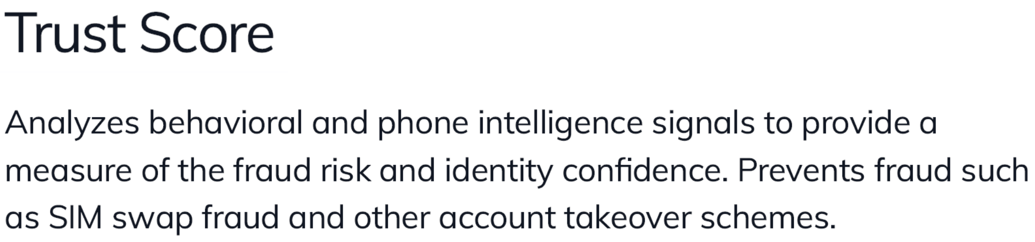
PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT

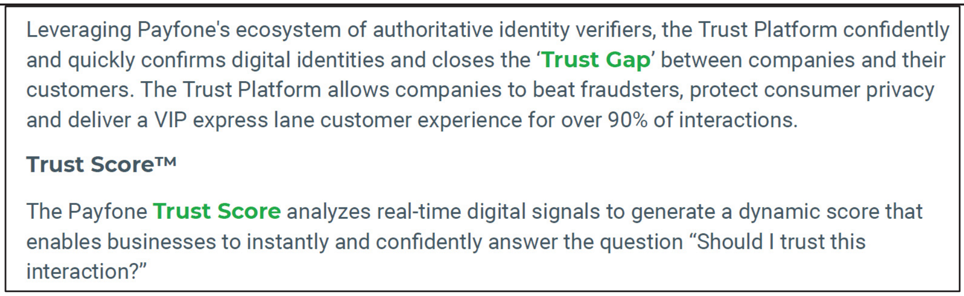
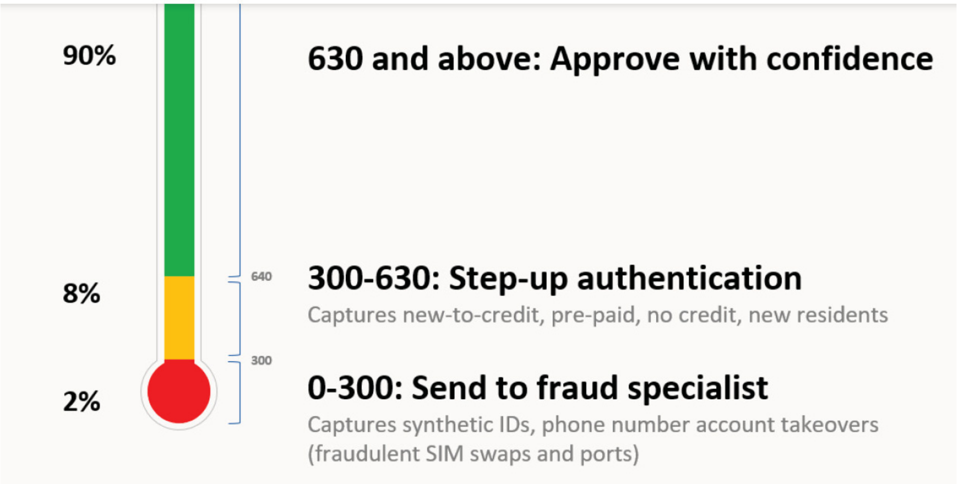
US 8,238,532 Claim 32

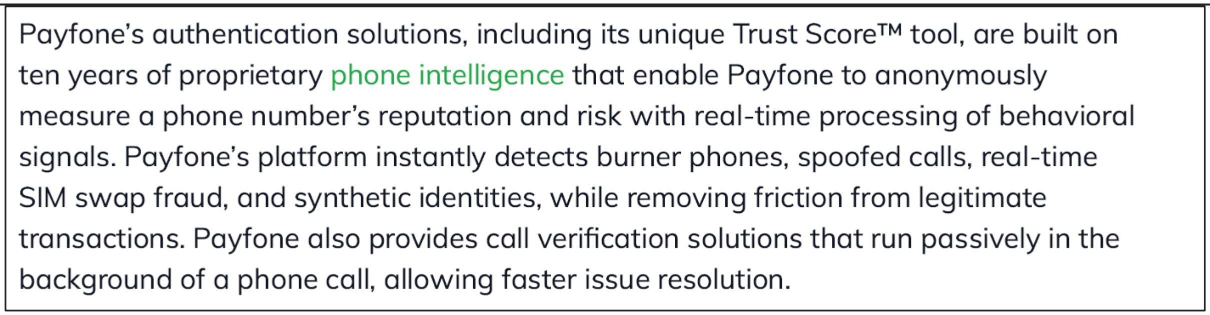
Prove's Call Center Authentication

32. A system for performing forensic analysis on calling party number information associated with an incoming call from a telephonic device, before the incoming call is answered, comprising:	Prove's Call Center Authentication performs "*forensic analysis on calling party number information*," (e.g., ANI), "*associated with an incoming call from a telephonic device*," e.g., call to a call center.  **Proactive call verification technology to stop fraud before it starts** Call Center Authentication is the world's first full-stack solution that enables enterprises to: • Preemptively protect their call centers against emerging threats such as IVR (interactive voice response) credential stuffing, ANI spoofing, SIM swap, and account takeover • Greenlight the majority of callers without subjecting them to frustrating roadblocks such as knowledge-based security questions or one-time passcodes Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience. *Exhibit 9 at 2.*

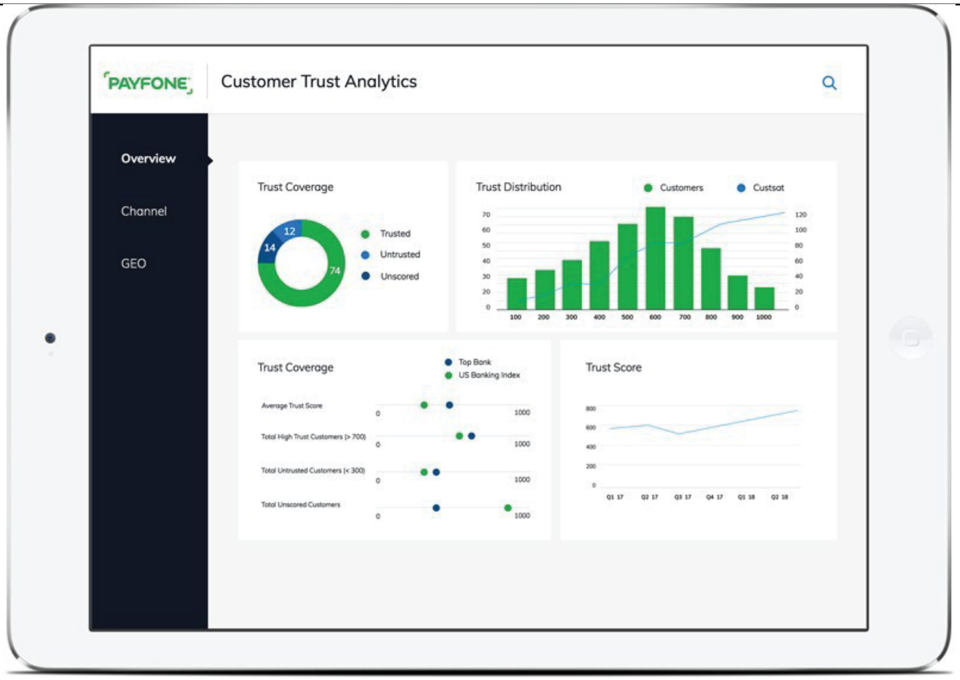
	 The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.* The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention. *Exhibit 10 at 1.*

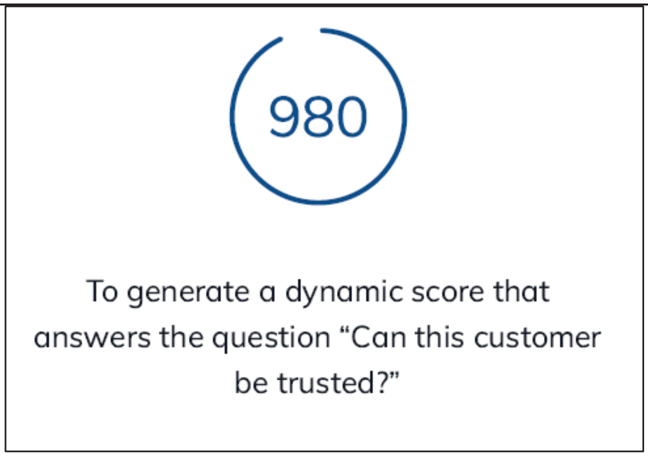
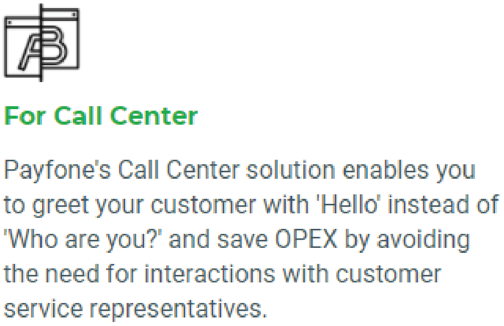
	 LET'S SEE LUCAS'S EXPERIENCE IN ACTION 1 The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone A week later, Lucas calls General Mortgage's 800 customer service number to update his address 2 3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now 4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions 5 Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?" *Exhibit 13 at 1.*  Trust Score Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes. *Exhibit 8 at 1-2.*

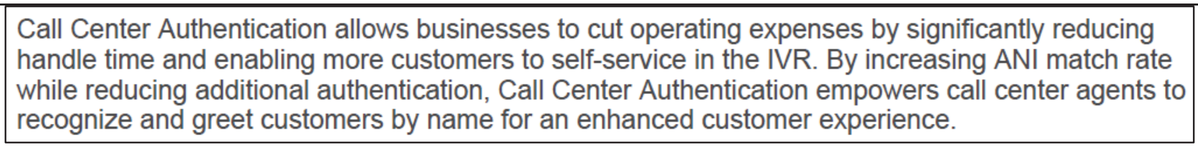
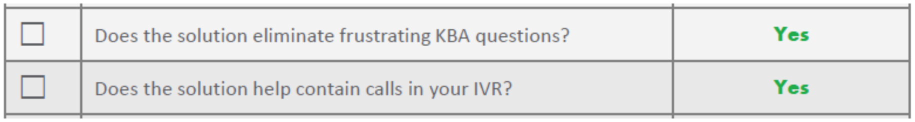
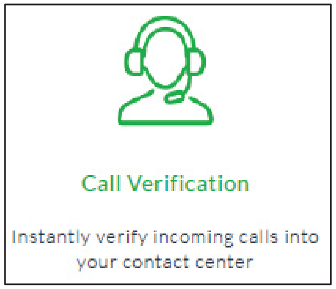
	 Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the '**Trust Gap**' between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions. **Trust Score™** The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question "Should I trust this interaction?" *Exhibit 11 at 4.*  **630 and above: Approve with confidence** **300-630: Step-up authentication** Captures new-to-credit, pre-paid, no credit, new residents **0-300: Send to fraud specialist** Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports) *Exhibit 11 at 5.*

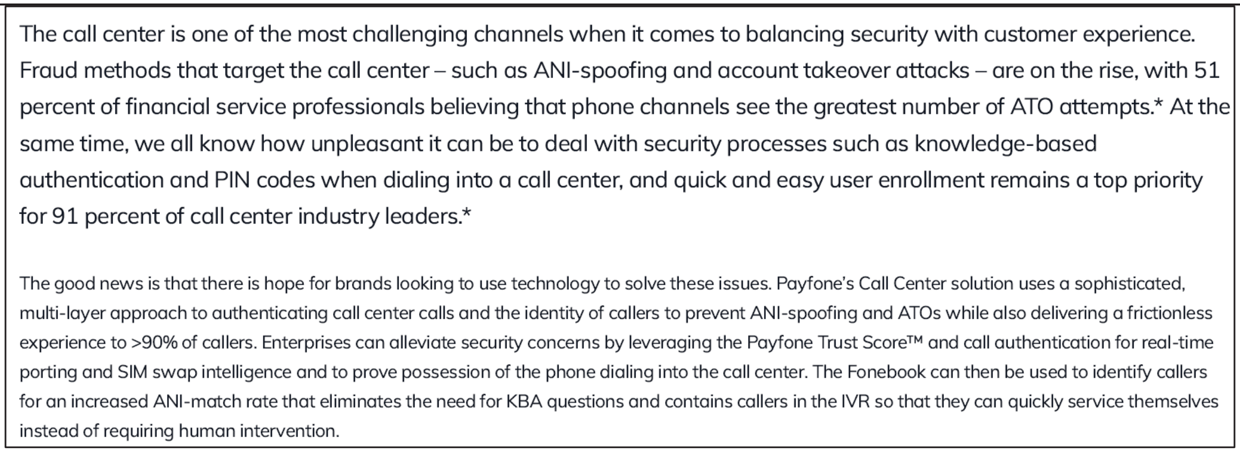
	 Payfone's authentication solutions, including its unique Trust Score™ tool, are built on ten years of proprietary phone intelligence that enable Payfone to anonymously measure a phone number's reputation and risk with real-time processing of behavioral signals. Payfone's platform instantly detects burner phones, spoofed calls, real-time SIM swap fraud, and synthetic identities, while removing friction from legitimate transactions. Payfone also provides call verification solutions that run passively in the background of a phone call, allowing faster issue resolution. *Exhibit 15 at 2*

**PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT**

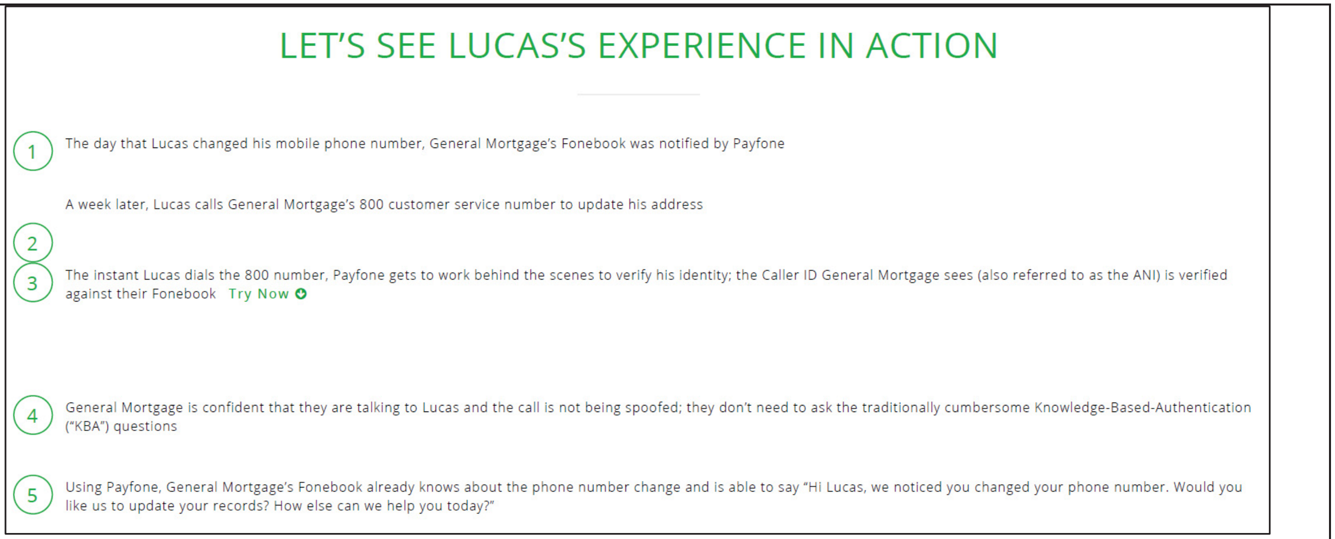
	 PAYFONE Customer Trust Analytics Overview Channel GEO Trust Coverage 12 14 74 Trusted Untrusted Unscored Trust Distribution Customers Custsat 70 60 50 40 30 20 0 120 100 80 60 40 20 0 100 200 300 400 500 600 700 800 900 1000 Trust Coverage Top Bank US Banking Index Average Trust Score Total High Trust Customers (> 700) Total Untrusted Customers (< 300) Total Unscored Customers 0 1000 Trust Score 800 600 400 200 0 Q1 17 Q2 17 Q3 17 Q4 17 Q1 18 Q2 18 *Exhibit 20 at 1.*

	 980 To generate a dynamic score that answers the question "Can this customer be trusted?" *Exhibit 17 at 3.* On information and belief, this "*forensic analysis*" is performed "*before the incoming call is answered*."  **For Call Center** Payfone's Call Center solution enables you to greet your customer with 'Hello' instead of 'Who are you?' and save OPEX by avoiding the need for interactions with customer service representatives. *Exhibit 11 at 3.*

	 Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience. *Exhibit 9 at 2.*  □ Does the solution eliminate frustrating KBA questions? Yes □ Does the solution help contain calls in your IVR? Yes *Exhibit 12 at 1.*  Call Verification Instantly verify incoming calls into your contact center *Exhibit 21 at 1.*
an interface for receiving calling party number information associated with the incoming call;	Prove's Call Center receives "*the calling party number information*" (e.g., SIP INVITE information and ANI).

	 The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.* The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention. *Exhibit 10 at 1.*

**PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT**



LET'S SEE LUCAS'S EXPERIENCE IN ACTION

1 The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone

2 A week later, Lucas calls General Mortgage's 800 customer service number to update his address

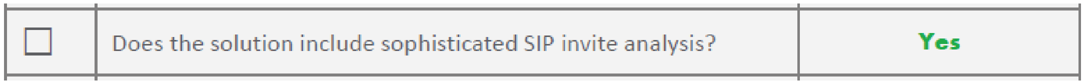
3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now

4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions

5 Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?"

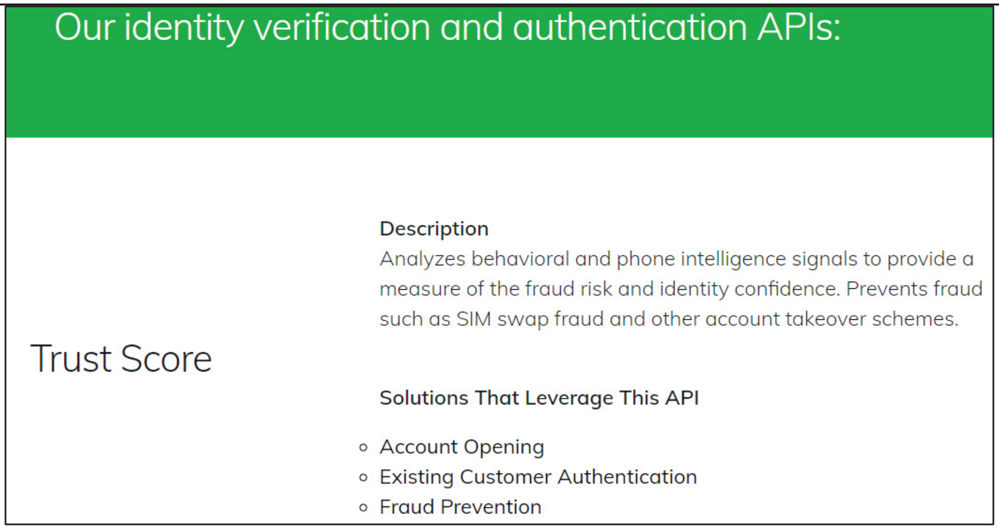
Exhibit 13 at 1.

On information and belief, Prove Call Center Authentication receives SIP invite information, including the ANI, via Prove's APIs (i.e., "*interface*").



□	Does the solution include sophisticated SIP invite analysis?	Yes

Exhibit 12 at 1.



Our identity verification and authentication APIs:

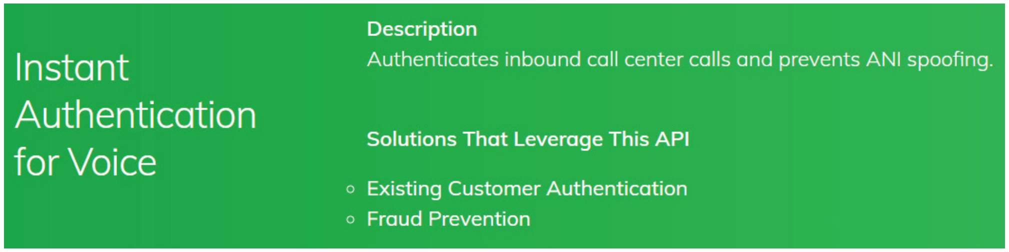
Trust Score

Description
Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes.

Solutions That Leverage This API

- Account Opening
- Existing Customer Authentication
- Fraud Prevention

Exhibit 8 at 2.



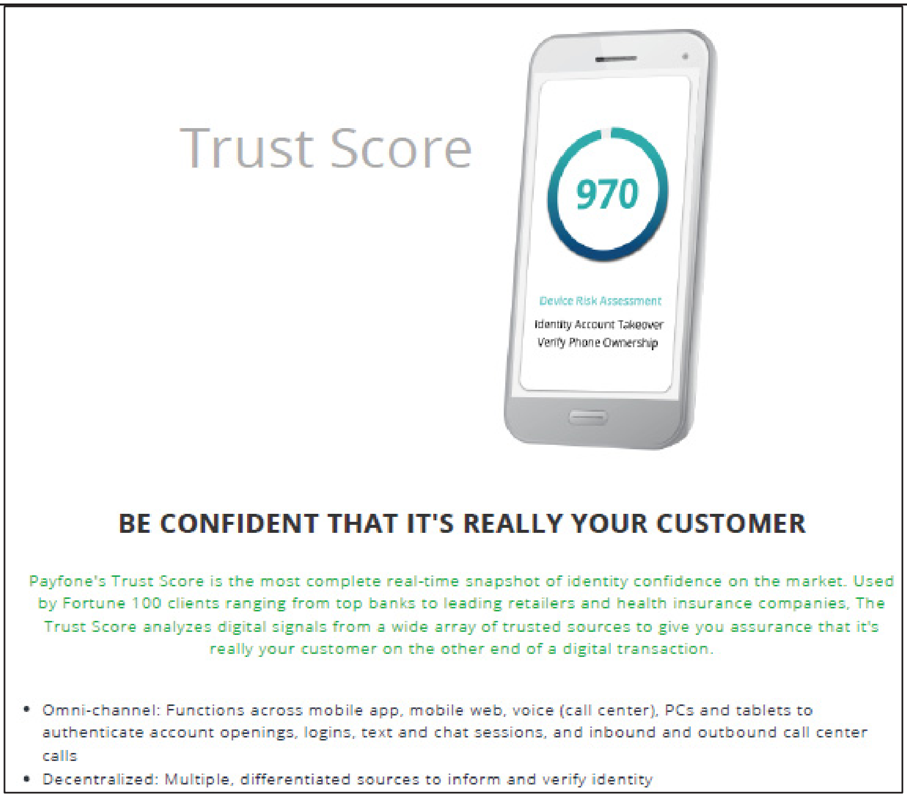
Instant Authentication for Voice

Description
Authenticates inbound call center calls and prevents ANI spoofing.

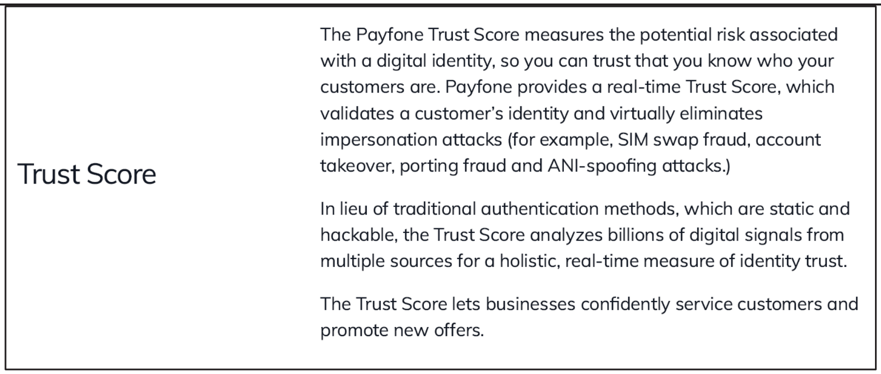
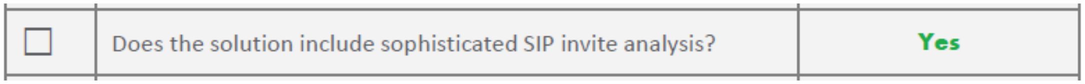
Solutions That Leverage This API

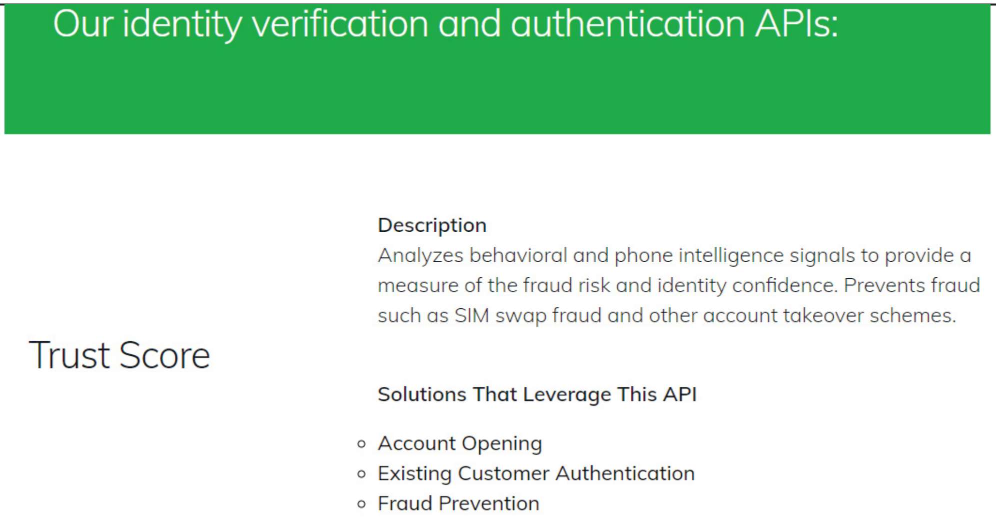
- Existing Customer Authentication
- Fraud Prevention

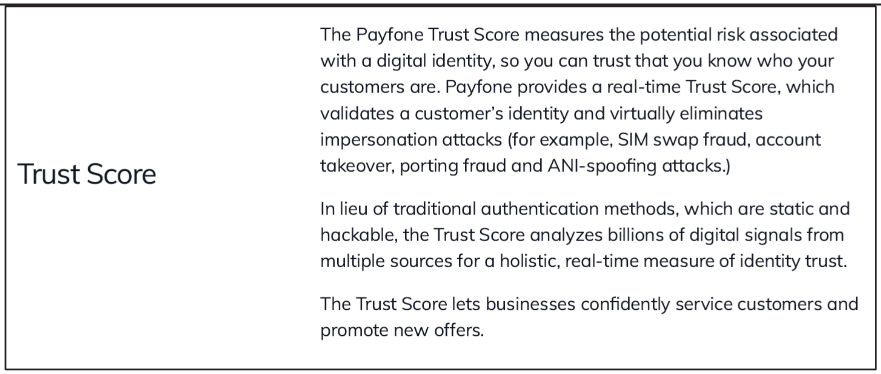
Exhibit 8 at 4.

	 970 Device Risk Assessment Identity Account Takeover Verify Phone Ownership Trust Score **BE CONFIDENT THAT IT'S REALLY YOUR CUSTOMER** Payfone's Trust Score is the most complete real-time snapshot of identity confidence on the market. Used by Fortune 100 clients ranging from top banks to leading retailers and health insurance companies, The Trust Score analyzes digital signals from a wide array of trusted sources to give you assurance that it's really your customer on the other end of a digital transaction. • Omni-channel: Functions across mobile app, mobile web, voice (call center), PCs and tablets to authenticate account openings, logins, text and chat sessions, and inbound and outbound call center calls • Decentralized: Multiple, differentiated sources to inform and verify identity *Exhibit 14 at 1.*
a memory configured to store a plurality of expected call patterns;	On information and belief, Prove's Call Center Authentication stores "*expected call patterns*" so that it can identify fraud such as SIM swap fraud, account takeover, porting fraud, and ANI-spoofing attacks based on the "billions of digital signals from multiple sources" that are analyzed.

**PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT**

	 Trust Score The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.) In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust. The Trust Score lets businesses confidently service customers and promote new offers. *Exhibit 17 at 3.*  □ Does the solution include sophisticated SIP invite analysis? Yes *Exhibit 12 at 1.*

	 Our identity verification and authentication APIs: Trust Score Description Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes. Solutions That Leverage This API ○ Account Opening ○ Existing Customer Authentication ○ Fraud Prevention *Exhibit 8 at 2.*
one or more processors configured to: gather operational status information associated with the calling party number information, and	Prove's Call Center Authentication gathers "*gather operational status information associated with the calling party number information*" (*e.g.*, "billions of digital signals from multiple sources," Fonebook).



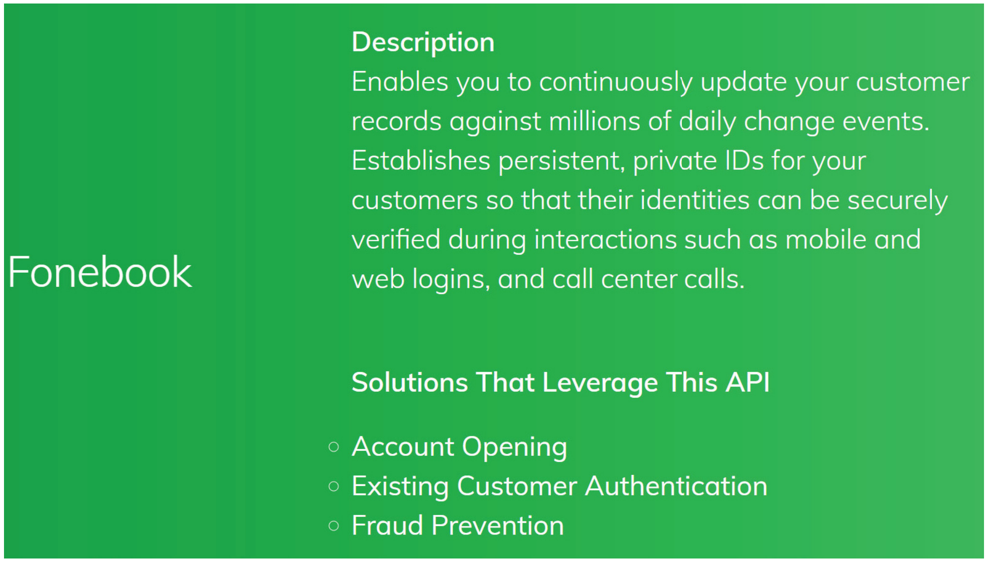
Trust Score

The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.)

In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust.

The Trust Score lets businesses confidently service customers and promote new offers.

Exhibit 17 at 3.



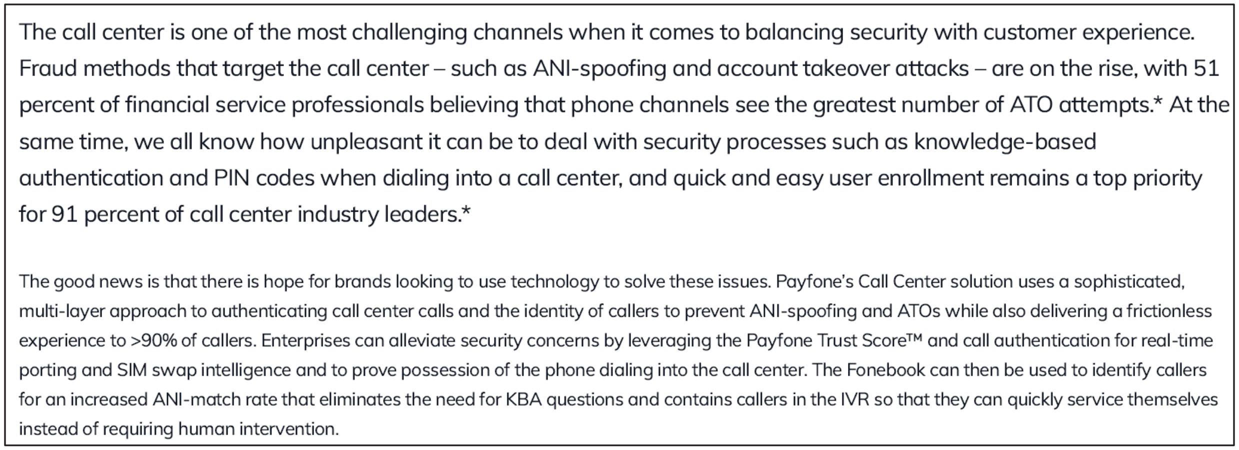
Fonebook

Description

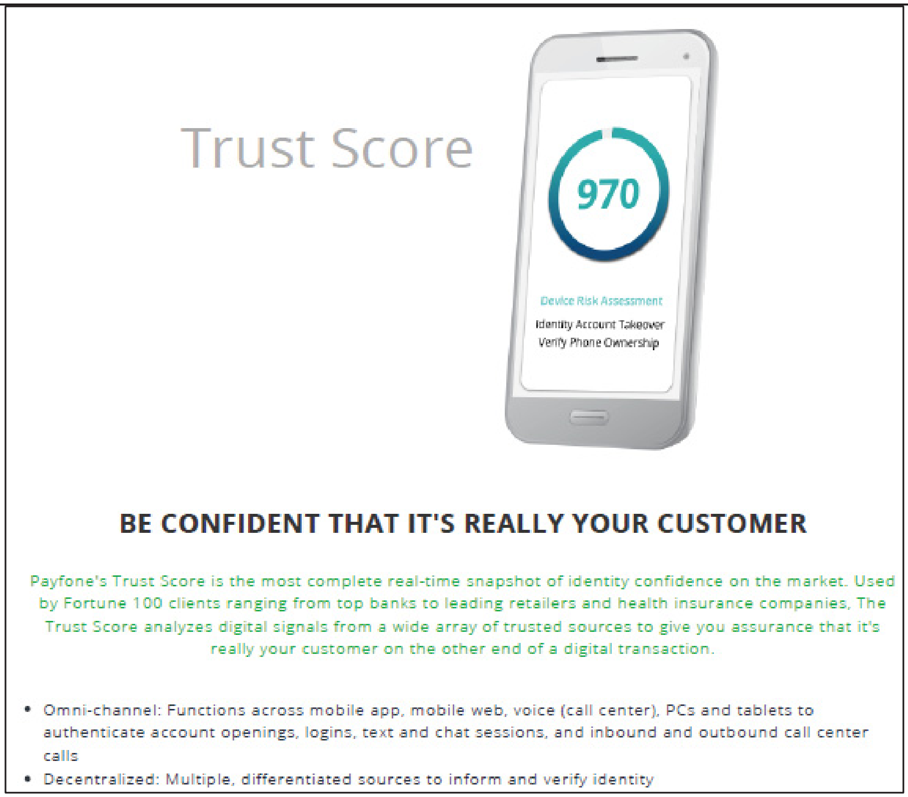
Enables you to continuously update your customer records against millions of daily change events. Establishes persistent, private IDs for your customers so that their identities can be securely verified during interactions such as mobile and web logins, and call center calls.

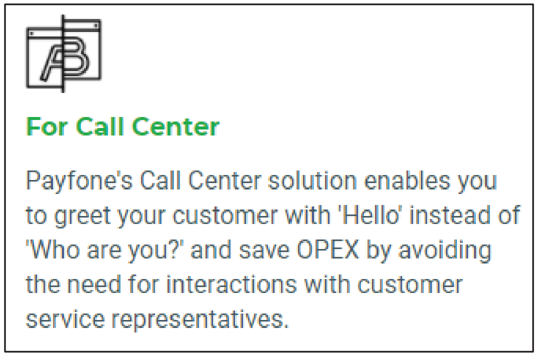
Solutions That Leverage This API

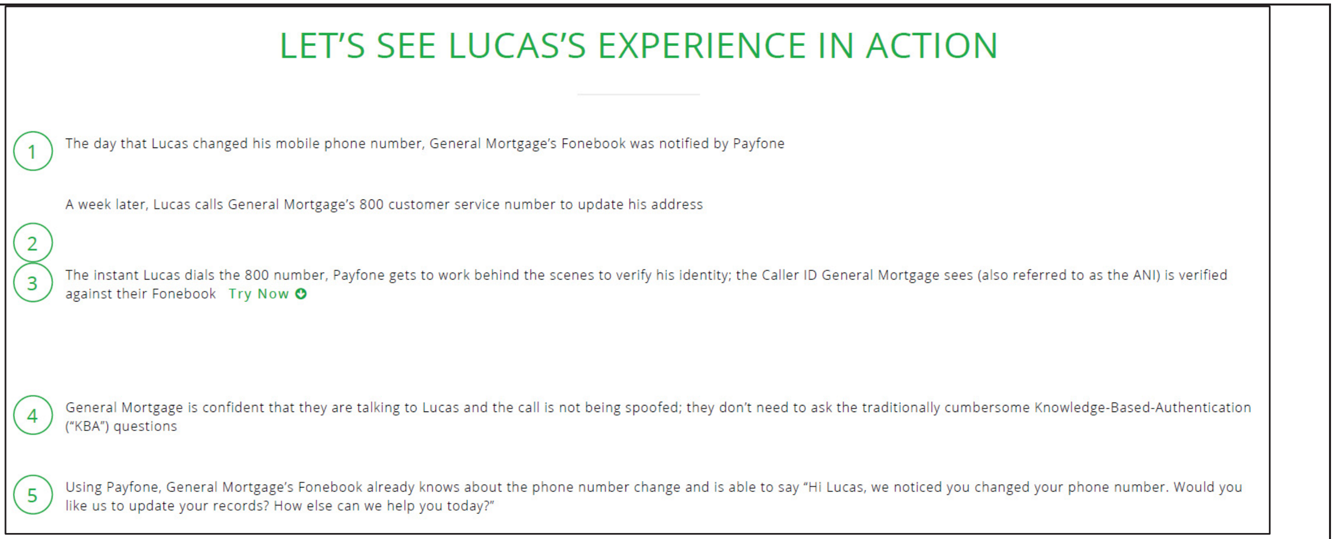
○ Account Opening
○ Existing Customer Authentication
○ Fraud Prevention

	Exhibit 8 at 2.  The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.* The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention. *Exhibit 10 at 1.*

PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT

	 Trust Score 970 Device Risk Assessment Identity Account Takeover Verify Phone Ownership **BE CONFIDENT THAT IT'S REALLY YOUR CUSTOMER** Payfone's Trust Score is the most complete real-time snapshot of identity confidence on the market. Used by Fortune 100 clients ranging from top banks to leading retailers and health insurance companies, The Trust Score analyzes digital signals from a wide array of trusted sources to give you assurance that it's really your customer on the other end of a digital transaction. • Omni-channel: Functions across mobile app, mobile web, voice (call center), PCs and tablets to authenticate account openings, logins, text and chat sessions, and inbound and outbound call center calls • Decentralized: Multiple, differentiated sources to inform and verify identity *Exhibit 14 at 1.* At a minimum, Rodger Desai indicated that Prove analyzes information such astenure of a number, behavior, and funding mechanism. *See* Consult Hyperion: Event 21 - Fireside Chat With Rodger Desai, *available at* https://chyp.com/webinars/week-21-fireside-chat-with-rodger-desai/. *See also* Payfone's Rodger Desai: Digital Transactions Should Be As Easy As Making A Phone Call, *available at https://tearsheet.co/podcasts/payfones-rodger-desai-digital-transactions-should-be-as-easy-as-making-a-phone-call/*

	On information and belief, the "*operational status information*" is gathered "*before the incoming call is answered*" because Prove instantly verifies calls.  For Call Center Payfone's Call Center solution enables you to greet your customer with 'Hello' instead of 'Who are you?' and save OPEX by avoiding the need for interactions with customer service representatives. *Exhibit 11 at 3.*



LET'S SEE LUCAS'S EXPERIENCE IN ACTION

1 The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone

A week later, Lucas calls General Mortgage's 800 customer service number to update his address

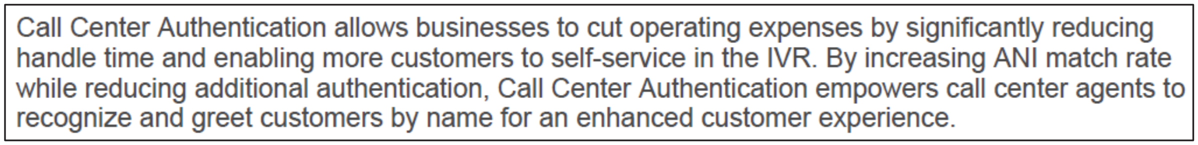
2

3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now

4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions

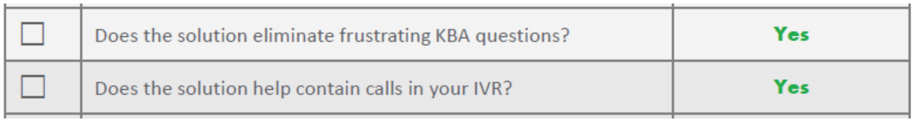
5 Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?"

Exhibit 13 at 1.



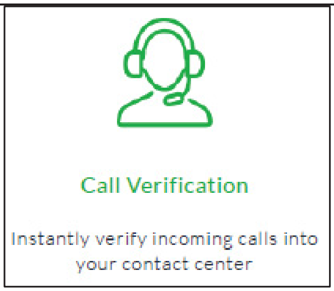
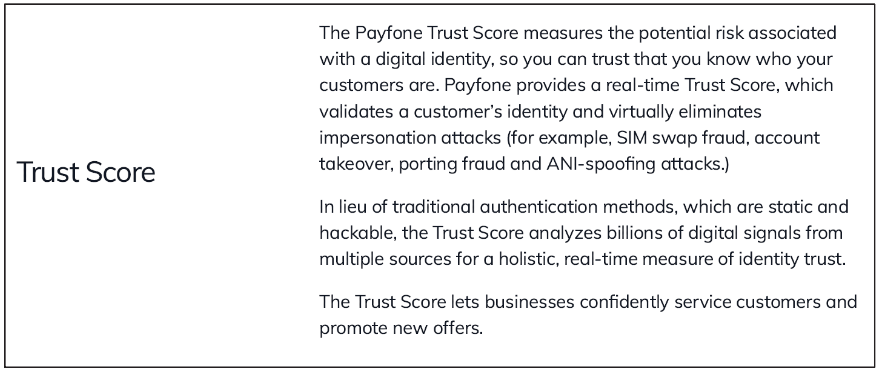
Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience.

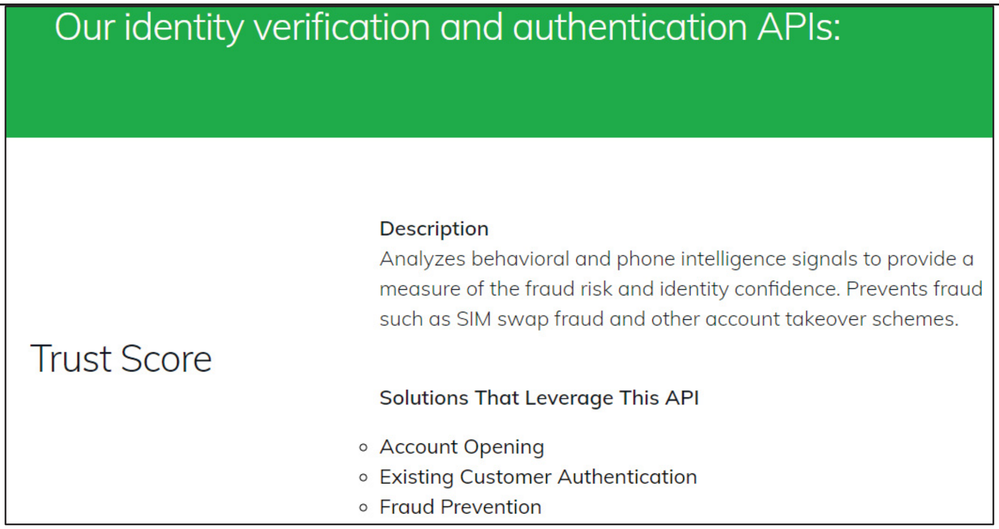
Exhibit 9 at 2.



□	Does the solution eliminate frustrating KBA questions?	Yes
□	Does the solution help contain calls in your IVR?	Yes

Exhibit 12 at 1.

	 Call Verification Instantly verify incoming calls into your contact center *Exhibit 21 at 1.*
assign a source origin confidence metric to the calling party number using the operational status information and an expected call pattern in the plurality of expected call patterns.	On information and belief, Prove's Call Center Authentication assigns a numeric Trust Score (i.e., "*source origin confidence metric*") to the calling party number based on the gathered "*operational status information*" and "*expected call patterns*," e.g., behavioral patterns.  Trust Score The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.) In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust. The Trust Score lets businesses confidently service customers and promote new offers. *Exhibit 17 at 3.*



Our identity verification and authentication APIs:

Trust Score

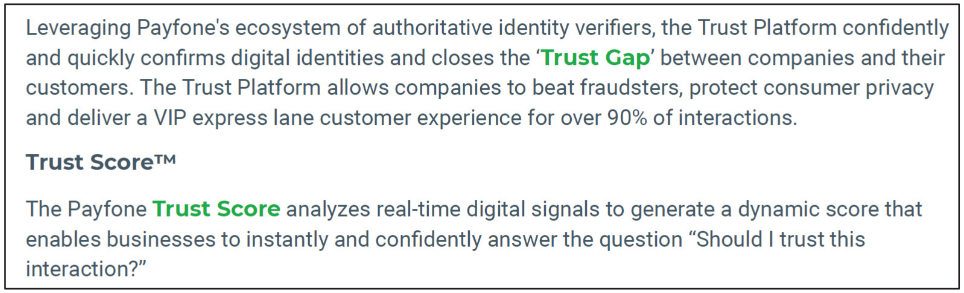
Description

Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes.

Solutions That Leverage This API

- Account Opening
- Existing Customer Authentication
- Fraud Prevention

Exhibit 8 at 2.

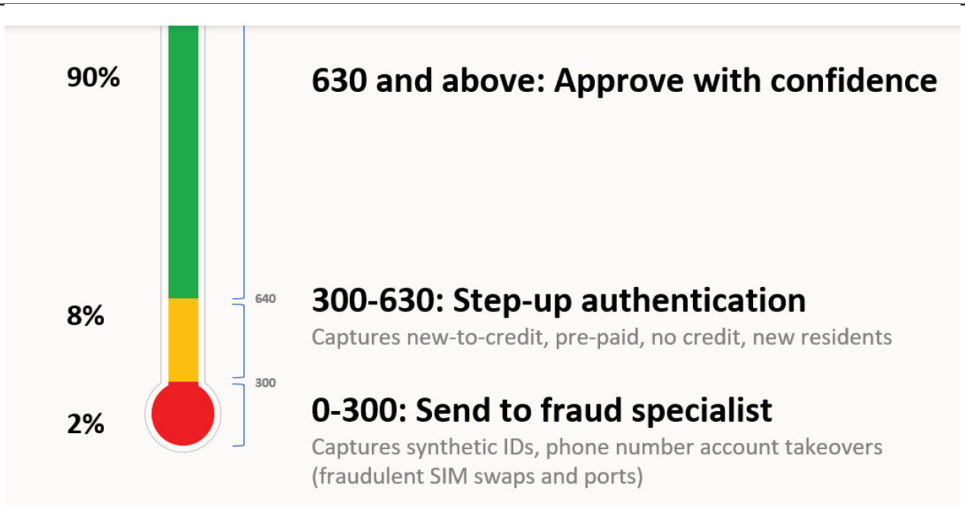


Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the '**Trust Gap**' between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions.

Trust Score™

The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question "Should I trust this interaction?"

Exhibit 11 at 4.

	 **630 and above: Approve with confidence** **300-630: Step-up authentication** Captures new-to-credit, pre-paid, no credit, new residents **0-300: Send to fraud specialist** Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports) *Exhibit 11 at 5.*

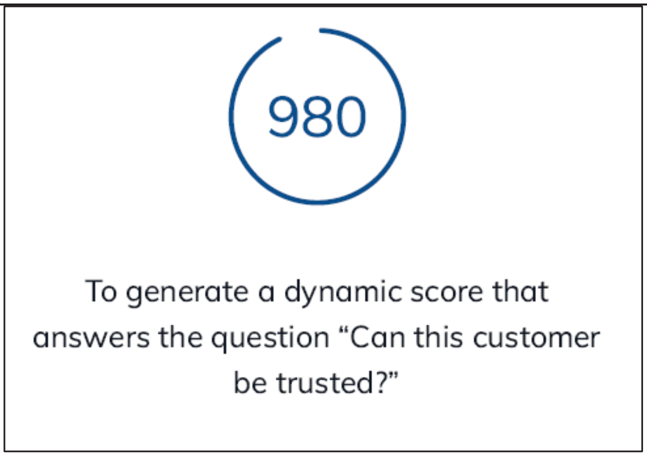
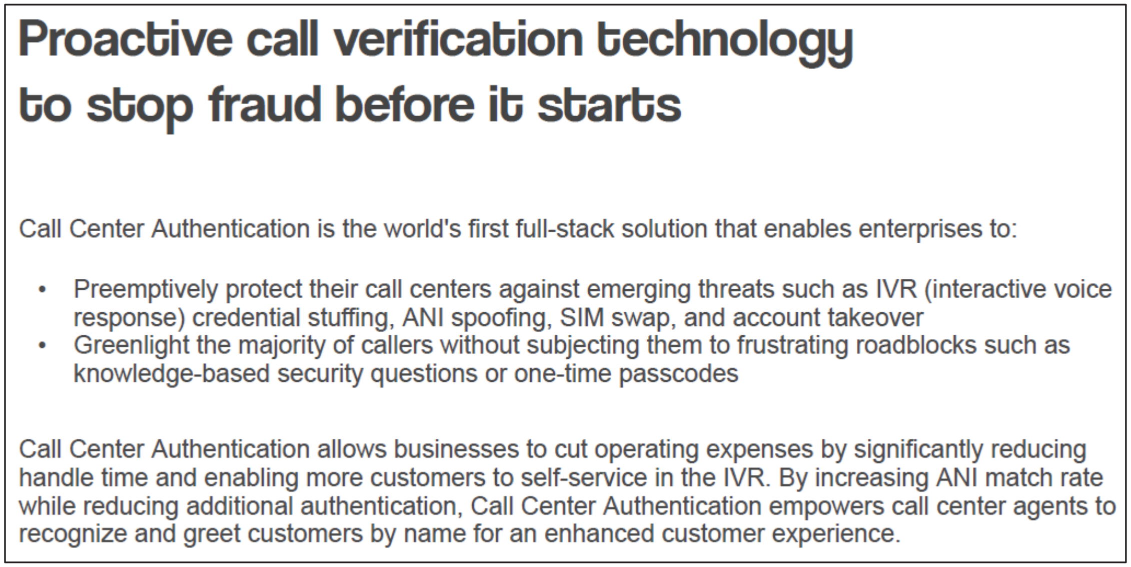
	 To generate a dynamic score that answers the question “Can this customer be trusted?” *Exhibit 17 at 3.*

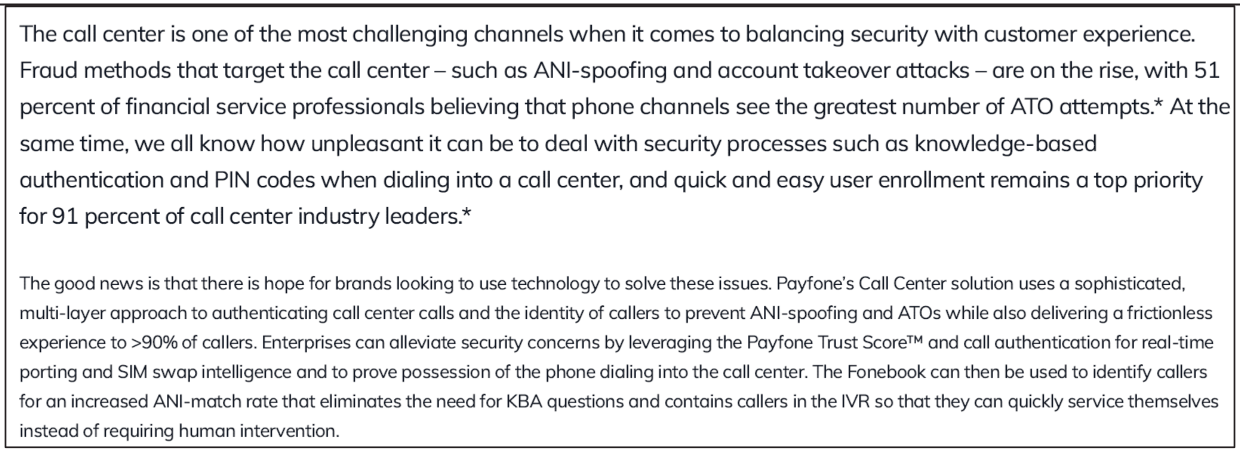
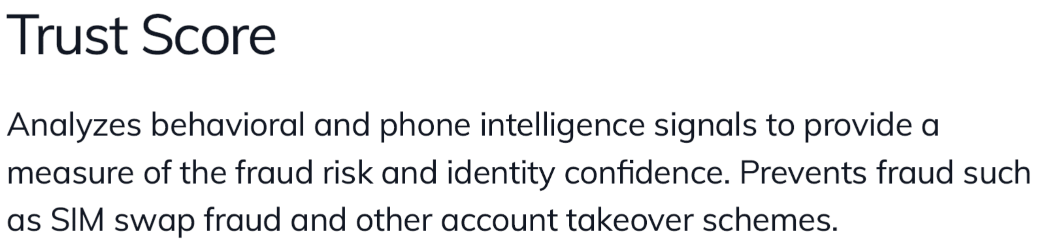
Exhibit 24

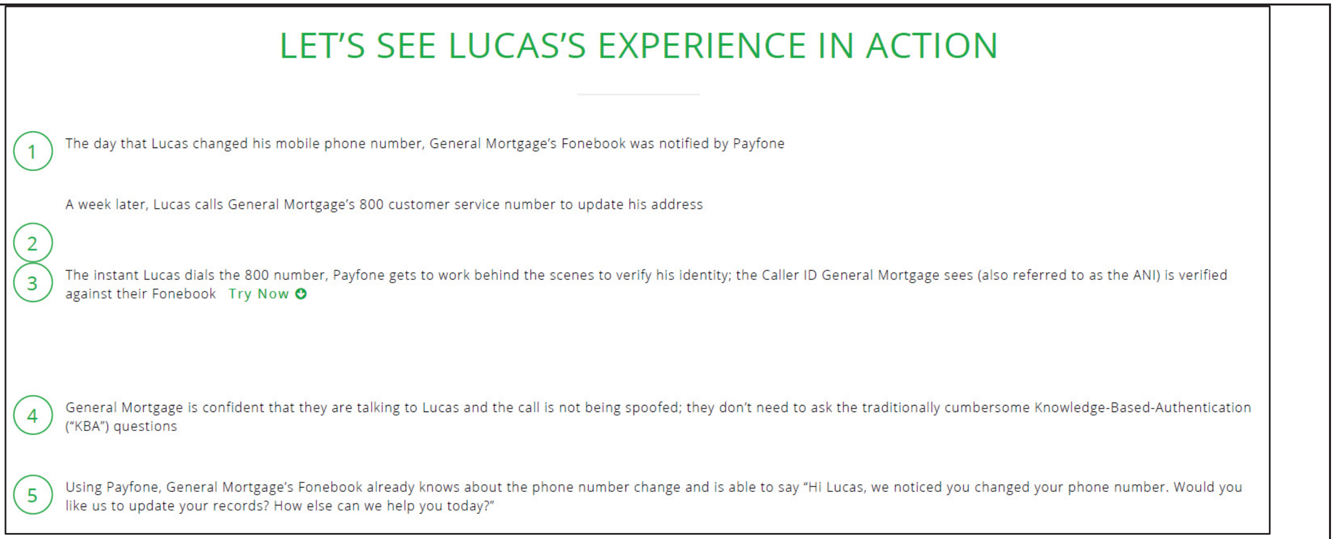
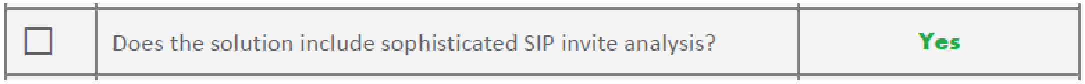
**PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT**

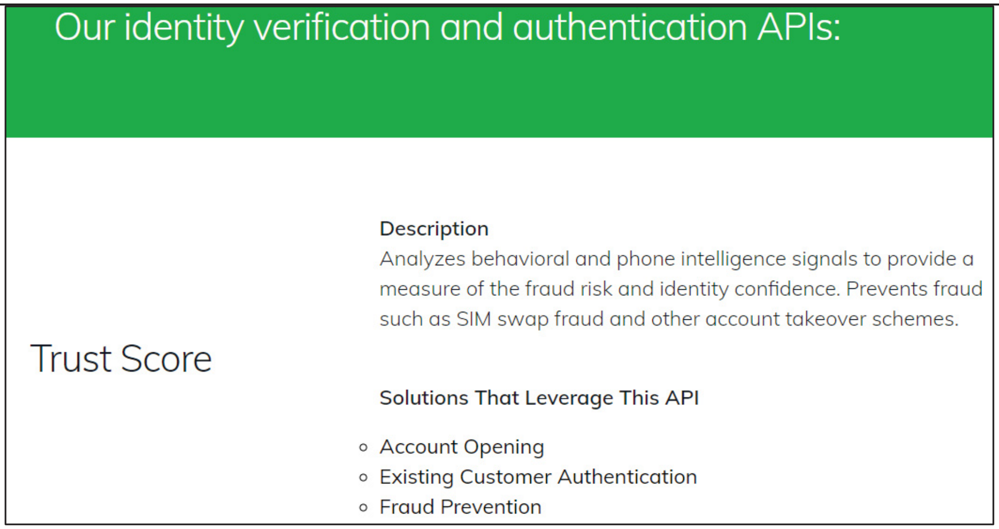
US 9,871,913 Claim 1

Prove's Call Center Authentication

1. A computer-implemented method, comprising:	On information and belief, Prove's Call Center Authentication includes a computer-implemented method that analyzes information associated with a call to detect fraud (i.e., discrepancies).  **Proactive call verification technology to stop fraud before it starts** Call Center Authentication is the world's first full-stack solution that enables enterprises to: • Preemptively protect their call centers against emerging threats such as IVR (interactive voice response) credential stuffing, ANI spoofing, SIM swap, and account takeover • Greenlight the majority of callers without subjecting them to frustrating roadblocks such as knowledge-based security questions or one-time passcodes Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience. *Exhibit 9 at 2.*

	 The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.* The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention. *Exhibit 10 at 1.*  Trust Score Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes. *Exhibit 8 at 1-2.*
receiving from a calling party by a discrepancy detector a call request having a called telephone number, wherein the call request includes calling party information, wherein the discrepancy detector determines discrepancies in calling party information and is ancillary to an originating service provider network element that provides a telephone line for	On information and belief, Prove's Call Center Authentication (the recited "*discrepancy detector*") receives "*a call request*" in the form of SIP INVITE information "*having a called telephone number, wherein the call request includes calling party information*," e.g., the customer service number dialed and the ANI received from the calling party.

the calling party placing the call request;	 LET'S SEE LUCAS'S EXPERIENCE IN ACTION 1 The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone A week later, Lucas calls General Mortgage's 800 customer service number to update his address 2 3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now 4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions 5 Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?" *Exhibit 13 at 1.*  □ Does the solution include sophisticated SIP invite analysis? Yes *Exhibit 12 at 1.*



Our identity verification and authentication APIs:

Trust Score

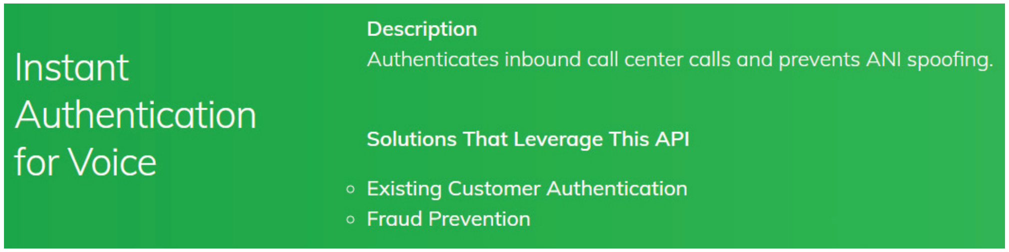
Description

Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes.

Solutions That Leverage This API

- Account Opening
- Existing Customer Authentication
- Fraud Prevention

Exhibit 8 at 2.



Instant Authentication for Voice

Description

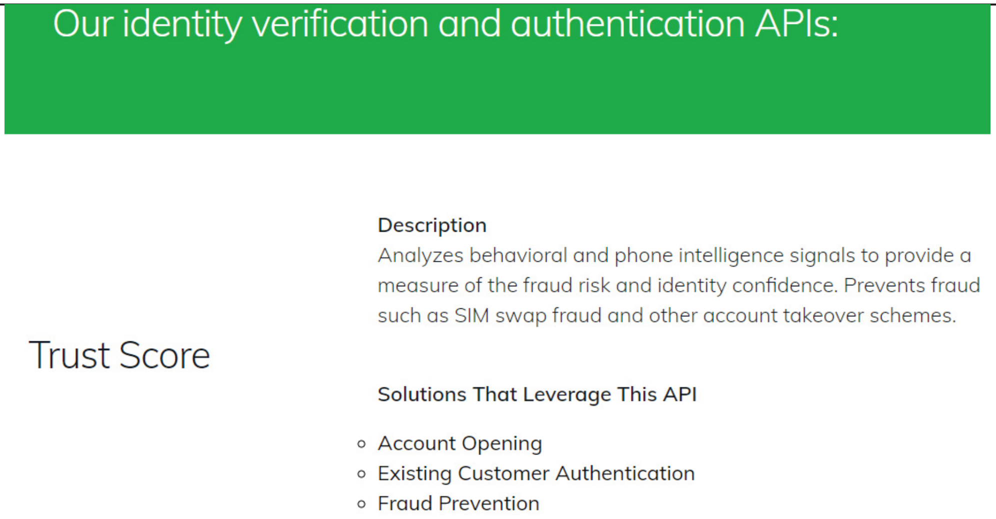
Authenticates inbound call center calls and prevents ANI spoofing.

Solutions That Leverage This API

- Existing Customer Authentication
- Fraud Prevention

Exhibit 8 at 4.

Prove's Call Center Authentication "determines discrepancies in calling party information" by analyzing "behavioral and phone intelligence signals" to detect fraud.



Our identity verification and authentication APIs:

Trust Score

Description

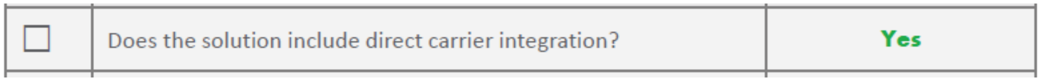
Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes.

Solutions That Leverage This API

- Account Opening
- Existing Customer Authentication
- Fraud Prevention

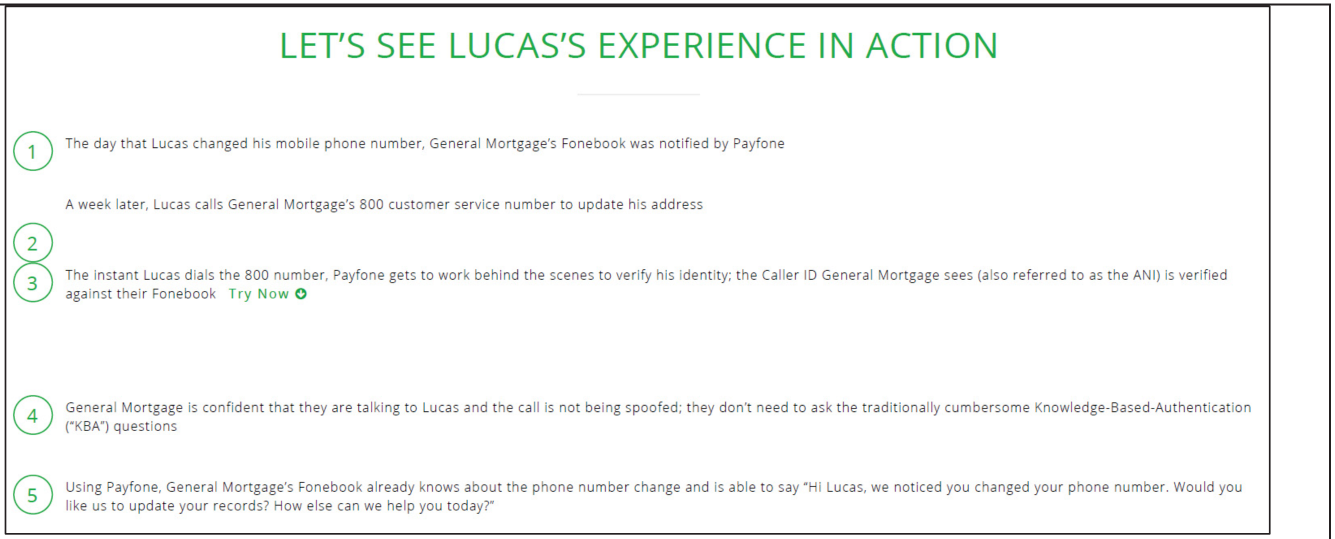
Exhibit 8 at 2.

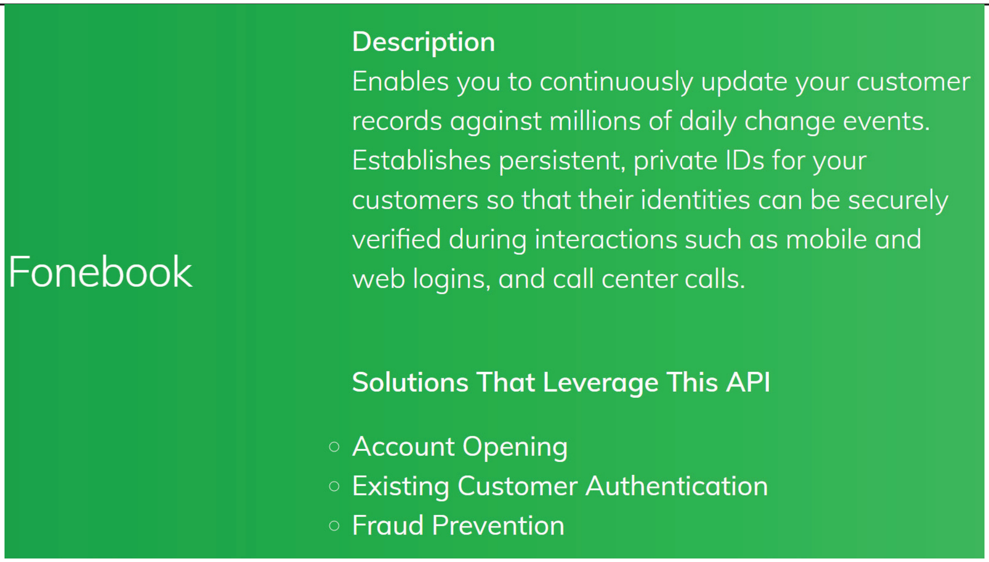
On information and belief, Prove's Call Center Authentication also "*is ancillary to an originating service provider network element that provides a telephone line for the calling party placing the call request.*"



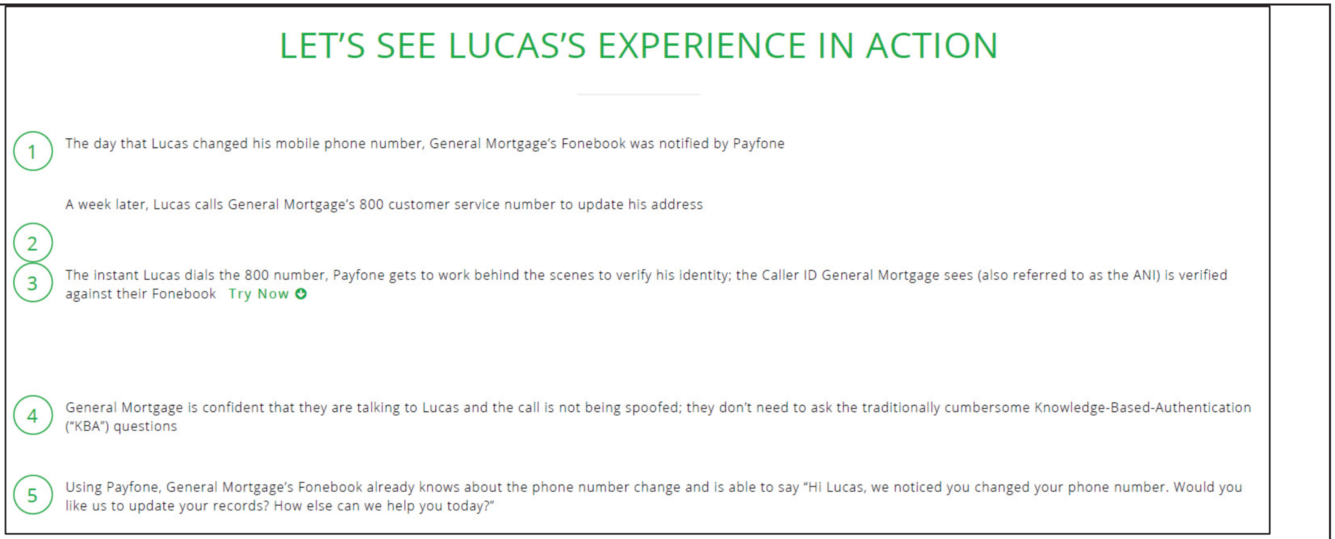
□	Does the solution include direct carrier integration?	Yes

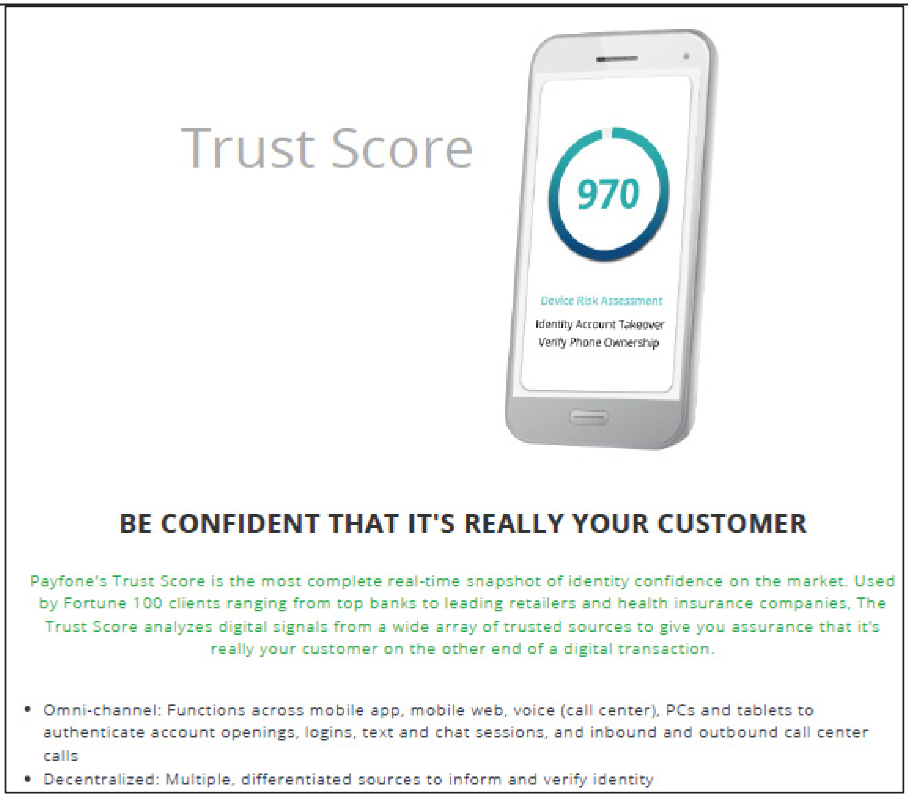
Exhibit 12 at 1.

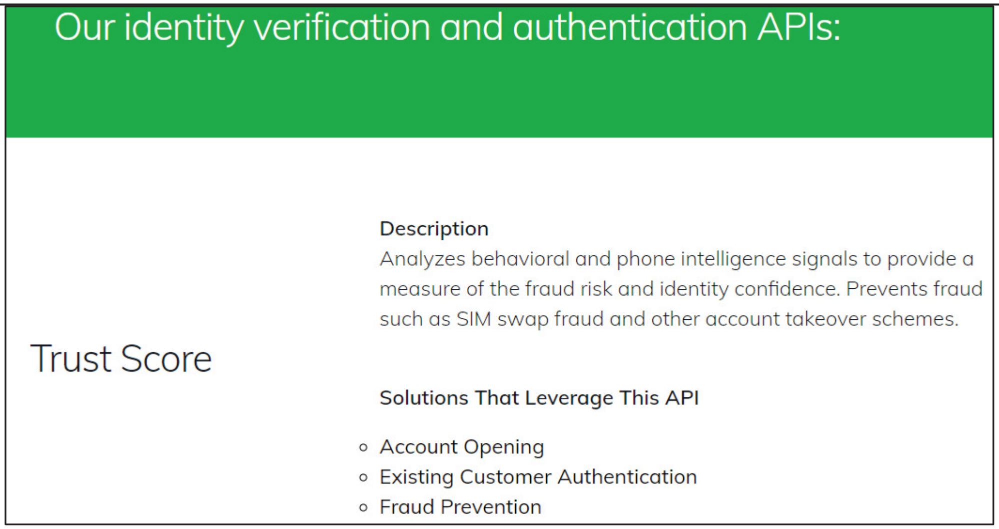
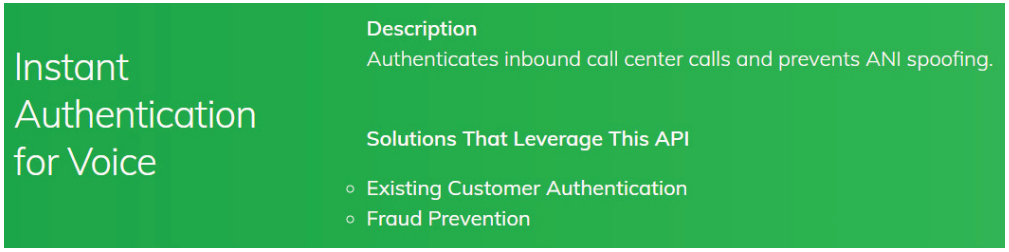
	 LET'S SEE LUCAS'S EXPERIENCE IN ACTION 1 The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone 2 A week later, Lucas calls General Mortgage's 800 customer service number to update his address 3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now 4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions 5 Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?" *Exhibit 13 at 1.*
accessing a monitored called party number database, wherein accessing the monitored called party number database includes determining whether the call request to the called telephone number is to be verified, wherein the monitored called party number database includes telephone numbers;	Direct Infringement: On information and belief, for outbound call center calls, Prove's Call Center Authentication accesses "*a monitored called party number database*," i.e., Fonebook, to determine whether a match can be found between the phone number received and an identity. If not further analysis is needed, i.e., "*determining whether the call request to the called telephone number is to be verified*." Fonebook includes telephone numbers associated with customer records.

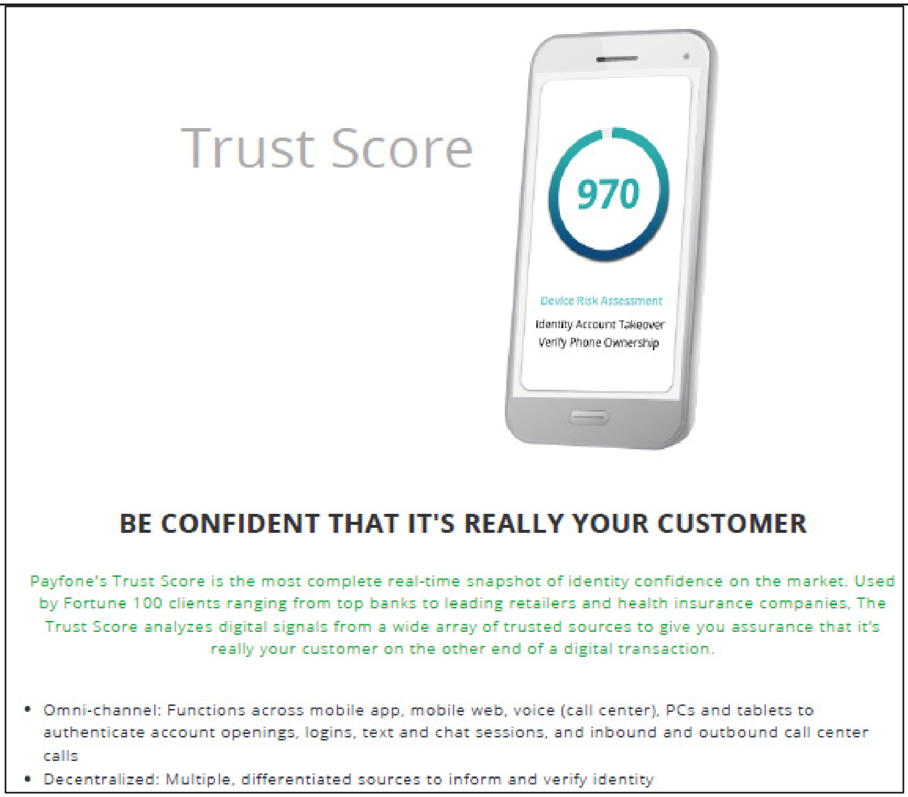
	 Fonebook **Description** Enables you to continuously update your customer records against millions of daily change events. Establishes persistent, private IDs for your customers so that their identities can be securely verified during interactions such as mobile and web logins, and call center calls. **Solutions That Leverage This API** ○ Account Opening ○ Existing Customer Authentication ○ Fraud Prevention *Exhibit 8 at 2.*

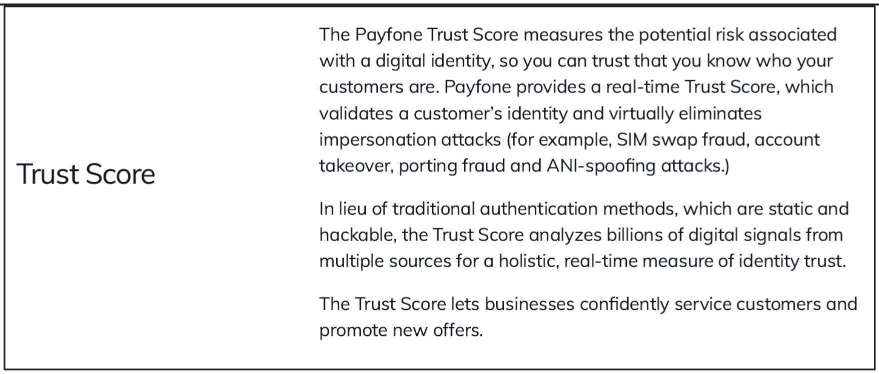
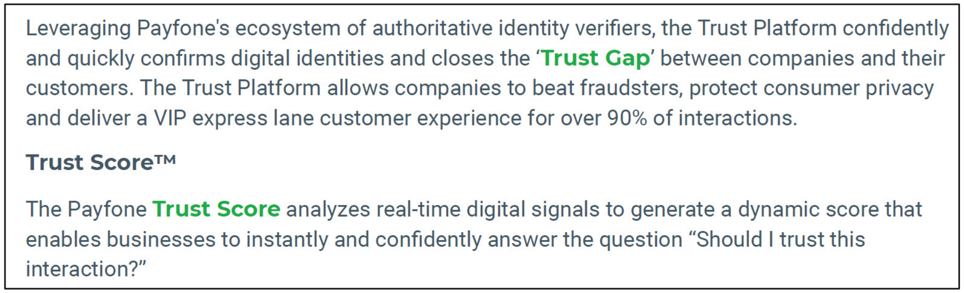
**PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT**

	 LET'S SEE LUCAS'S EXPERIENCE IN ACTION 1 The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone 2 A week later, Lucas calls General Mortgage's 800 customer service number to update his address 3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now 4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions 5 Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?" *Exhibit 13 at 1.*

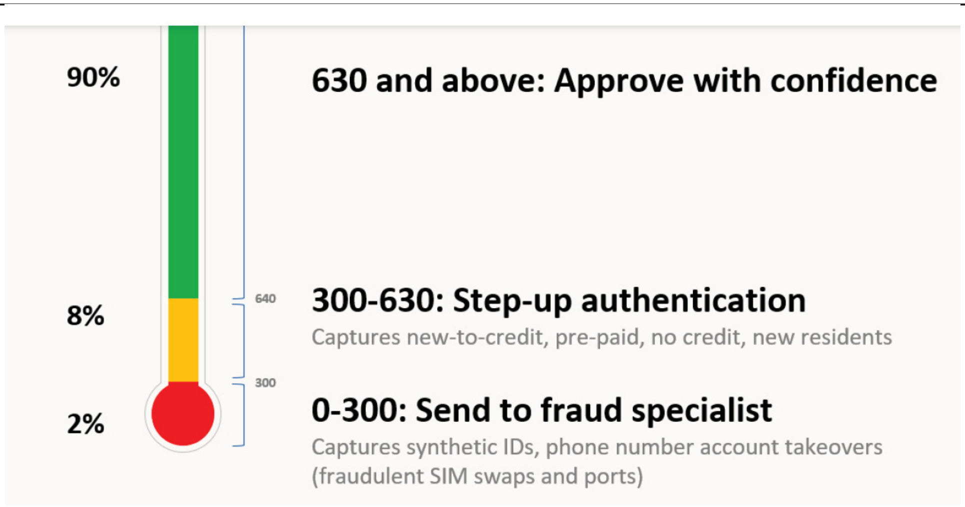
	 Trust Score 970 Device Risk Assessment Identity Account Takeover Verify Phone Ownership **BE CONFIDENT THAT IT'S REALLY YOUR CUSTOMER** Payfone's Trust Score is the most complete real-time snapshot of identity confidence on the market. Used by Fortune 100 clients ranging from top banks to leading retailers and health insurance companies. The Trust Score analyzes digital signals from a wide array of trusted sources to give you assurance that it's really your customer on the other end of a digital transaction. • Omni-channel: Functions across mobile app, mobile web, voice (call center), PCs and tablets to authenticate account openings, logins, text and chat sessions, and inbound and outbound call center calls • Decentralized: Multiple, differentiated sources to inform and verify identity *Exhibit 14 at 1.* Indirect Infringement: On information and belief, Prove's customers "*access[] a monitored called party number database*" to determine whether a call into a call center needs to be verified, e.g., based on the 800 number dialed. Prove's Call Center Authentication provides a set of APIs enabling its customers to invoke Prove's authentication.

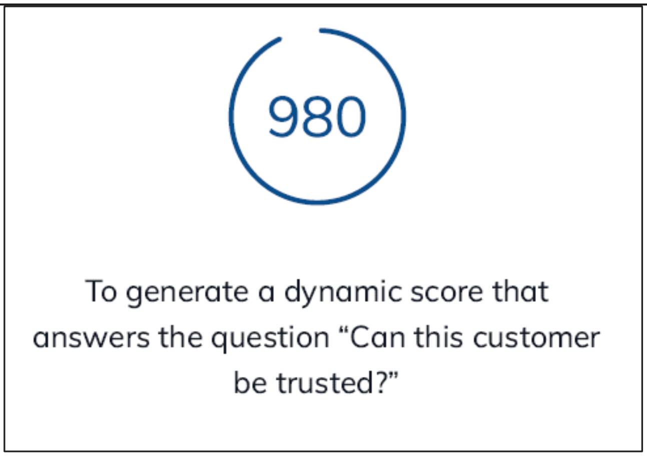
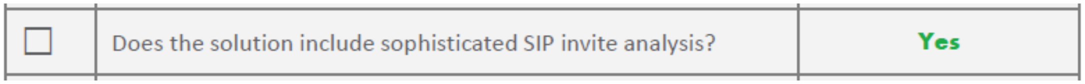
	 Our identity verification and authentication APIs: Trust Score Description Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes. Solutions That Leverage This API ○ Account Opening ○ Existing Customer Authentication ○ Fraud Prevention *Exhibit 8 at 2.*  Instant Authentication for Voice Description Authenticates inbound call center calls and prevents ANI spoofing. Solutions That Leverage This API ○ Existing Customer Authentication ○ Fraud Prevention *Exhibit 8 at 4.*

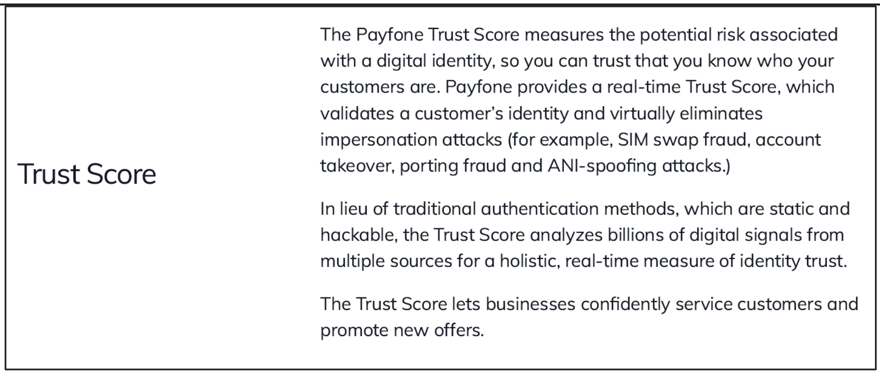
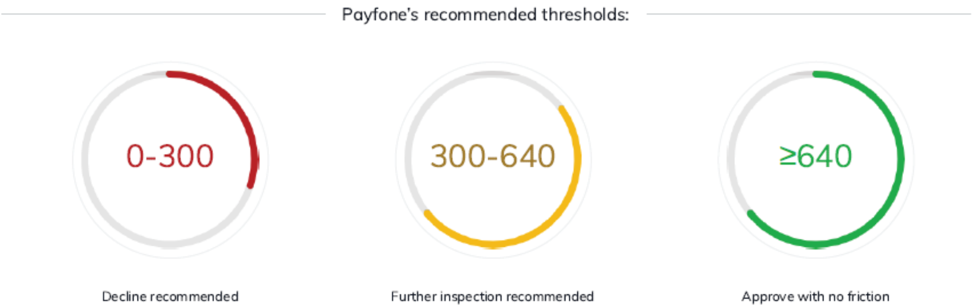
	 Trust Score 970 Device Risk Assessment Identity Account Takeover Verify Phone Ownership **BE CONFIDENT THAT IT'S REALLY YOUR CUSTOMER** Payfone's Trust Score is the most complete real-time snapshot of identity confidence on the market. Used by Fortune 100 clients ranging from top banks to leading retailers and health insurance companies, The Trust Score analyzes digital signals from a wide array of trusted sources to give you assurance that it's really your customer on the other end of a digital transaction. • Omni-channel: Functions across mobile app, mobile web, voice (call center), PCs and tablets to authenticate account openings, logins, text and chat sessions, and inbound and outbound call center calls • Decentralized: Multiple, differentiated sources to inform and verify identity *Exhibit 14 at 1.*
when the call request is to be verified, determining by the discrepancy detector whether a discrepancy exists between the calling party information contained within the call request and stored calling party information;	On information and belief, Prove's Call Center Authentication determines "*whether a discrepancy exists between the calling party information contained within the call request and stored calling party information*" in the form of a Trust Score.

	 Trust Score The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.) In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust. The Trust Score lets businesses confidently service customers and promote new offers. *Exhibit 17 at 3.*  Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the '**Trust Gap**' between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions. **Trust Score™** The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question "Should I trust this interaction?" *Exhibit 11 at 4.*

PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT

	 **630 and above: Approve with confidence** **300-630: Step-up authentication** Captures new-to-credit, pre-paid, no credit, new residents **0-300: Send to fraud specialist** Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports) *Exhibit 11 at 5.*

	 980 To generate a dynamic score that answers the question “Can this customer be trusted?” *Exhibit 17 at 3.* On information and belief, as part of its analysis, Prove’s Call Center Authentication compares SIP INVITE information (i.e., *information contained within the call request*”) to Fonebook information and “billions of digital signals from multiple sources” (i.e, “*stored calling party information*”).  □ Does the solution include sophisticated SIP invite analysis? **Yes** *Exhibit 12 at 1.*

	 Trust Score The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.) In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust. The Trust Score lets businesses confidently service customers and promote new offers. *Exhibit 17 at 3.*
when a discrepancy exists between the calling party information contained within the call request and stored calling party information, causing call processing of a call requested in the call request to be suspended.	On information and belief, Prove's Call Center Authentication "caus[es] call processing of a call requested in the call request to be suspended" by declining to proceed or sending to a fraud specialist for further inspection.  Payfone's recommended thresholds: 0-300 300-640 ≥640 Decline recommended Further inspection recommended Approve with no friction *Exhibit 17 at 3.*

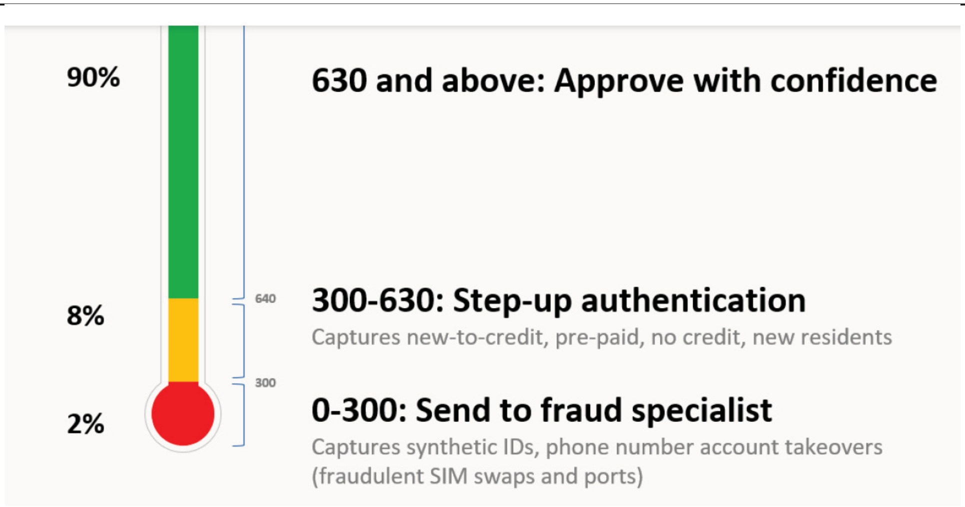
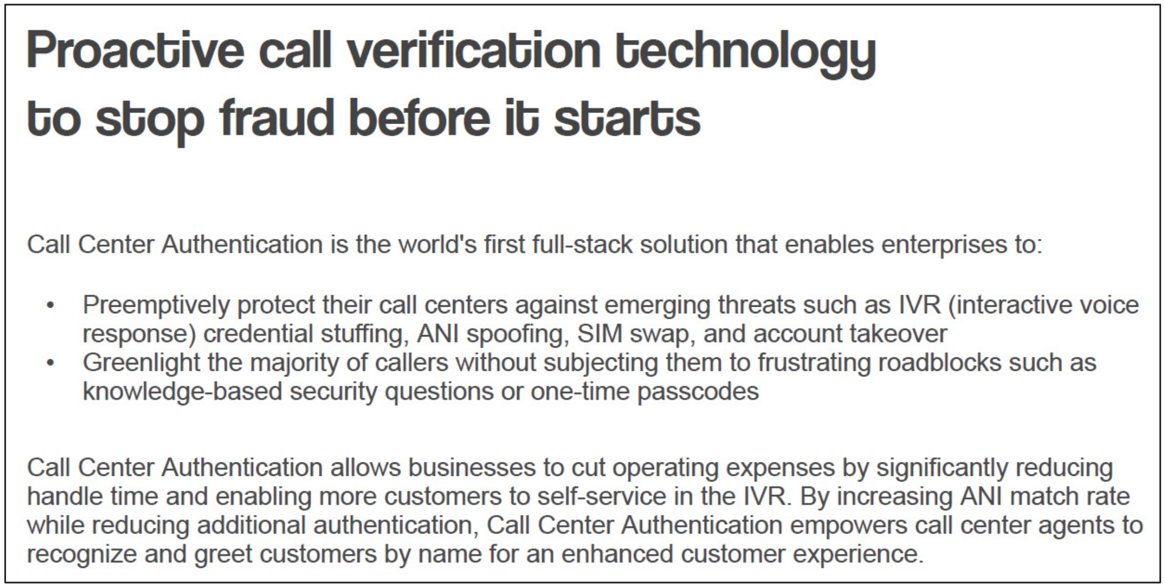
	 **630 and above: Approve with confidence** **300-630: Step-up authentication** Captures new-to-credit, pre-paid, no credit, new residents **0-300: Send to fraud specialist** Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports) *Exhibit 11 at 5.*

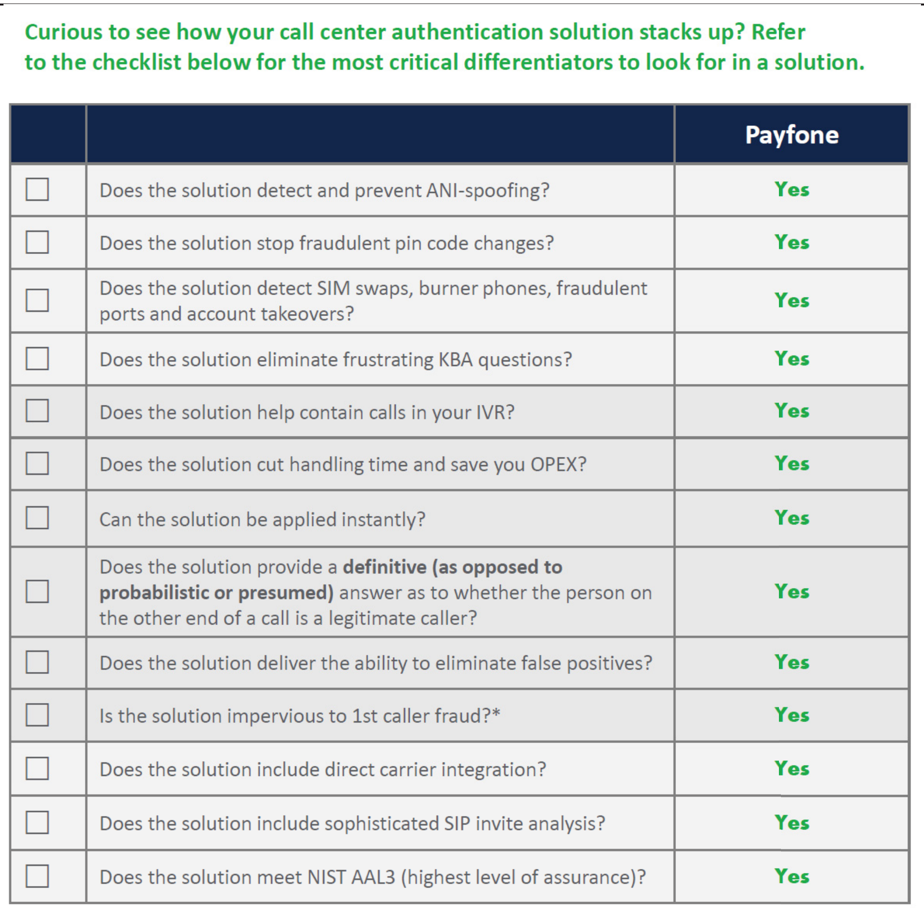
Exhibit 25

PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT

US 9,762,728 Claim 1

Prove's Call Center Authentication

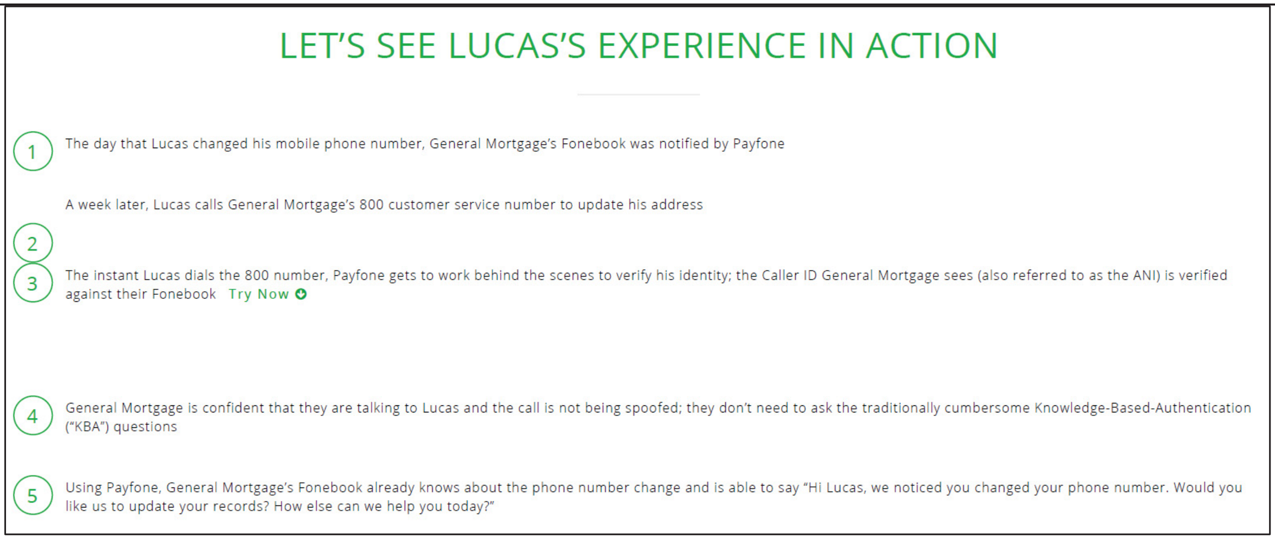
1. A method, comprising: receiving, by an authentication device, a call request and associated calling party information that includes a calling party number, wherein the call request is initiated by a caller;	On information and belief, Prove's Call Center Authentication includes a method comprising receiving a call request and associated calling party information (e.g., ANI) that includes a calling party number, wherein the call request is initiated by a caller.  **Proactive call verification technology to stop fraud before it starts** Call Center Authentication is the world's first full-stack solution that enables enterprises to: • Preemptively protect their call centers against emerging threats such as IVR (interactive voice response) credential stuffing, ANI spoofing, SIM swap, and account takeover • Greenlight the majority of callers without subjecting them to frustrating roadblocks such as knowledge-based security questions or one-time passcodes Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience. *Exhibit 9 at 2.*



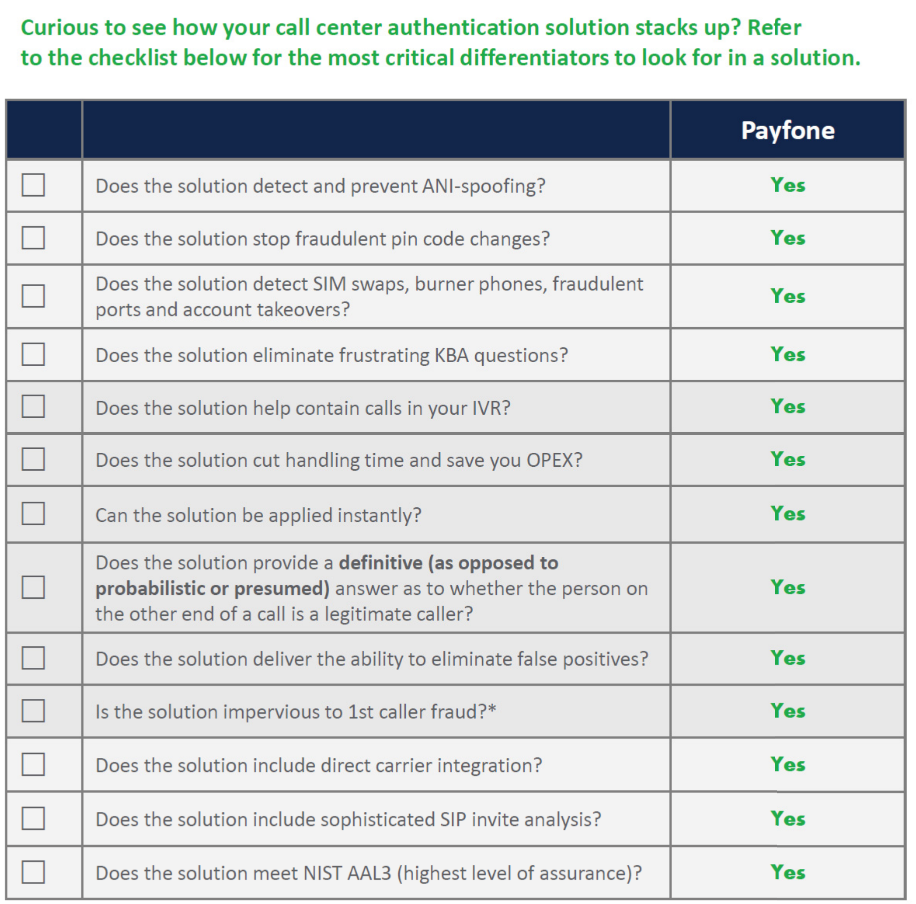
Curious to see how your call center authentication solution stacks up? Refer to the checklist below for the most critical differentiators to look for in a solution.

		Payfone
□	Does the solution detect and prevent ANI-spoofing?	Yes
□	Does the solution stop fraudulent pin code changes?	Yes
□	Does the solution detect SIM swaps, burner phones, fraudulent ports and account takeovers?	Yes
□	Does the solution eliminate frustrating KBA questions?	Yes
□	Does the solution help contain calls in your IVR?	Yes
□	Does the solution cut handling time and save you OPEX?	Yes
□	Can the solution be applied instantly?	Yes
□	Does the solution provide a **definitive (as opposed to probabilistic or presumed)** answer as to whether the person on the other end of a call is a legitimate caller?	Yes
□	Does the solution deliver the ability to eliminate false positives?	Yes
□	Is the solution impervious to 1st caller fraud?*	Yes
□	Does the solution include direct carrier integration?	Yes
□	Does the solution include sophisticated SIP invite analysis?	Yes
□	Does the solution meet NIST AAL3 (highest level of assurance)?	Yes

Exhibit 12 at 1.

	 LET’S SEE LUCAS’S EXPERIENCE IN ACTION 1 The day that Lucas changed his mobile phone number, General Mortgage’s Fonebook was notified by Payfone A week later, Lucas calls General Mortgage’s 800 customer service number to update his address 2 3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now 4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don’t need to ask the traditionally cumbersome Knowledge-Based-Authentication (“KBA”) questions 5 Using Payfone, General Mortgage’s Fonebook already knows about the phone number change and is able to say “Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?” *Exhibit 13 at 1.*
retrieving, by the authentication device, parameters associated with the calling party number, wherein the parameters include a number of accounts linked to the calling party number;	On information and belief, Prove’s Call Center Authentication retrieves parameters associated with the calling party number, wherein the parameters include a number of accounts linked to the calling party number.

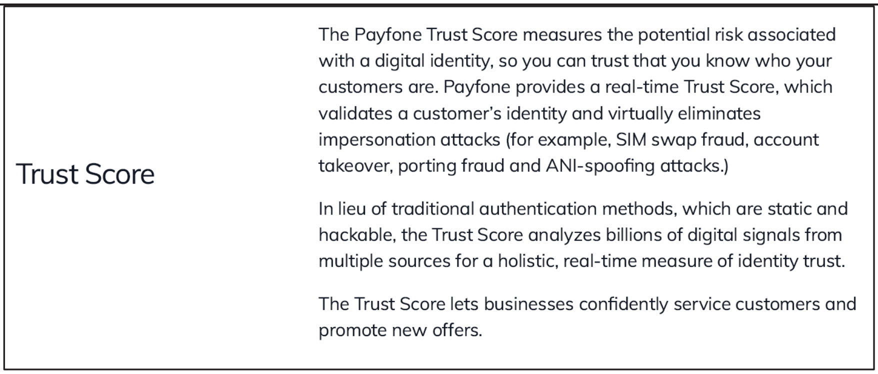
PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT



Curious to see how your call center authentication solution stacks up? Refer to the checklist below for the most critical differentiators to look for in a solution.

		Payfone
□	Does the solution detect and prevent ANI-spoofing?	Yes
□	Does the solution stop fraudulent pin code changes?	Yes
□	Does the solution detect SIM swaps, burner phones, fraudulent ports and account takeovers?	Yes
□	Does the solution eliminate frustrating KBA questions?	Yes
□	Does the solution help contain calls in your IVR?	Yes
□	Does the solution cut handling time and save you OPEX?	Yes
□	Can the solution be applied instantly?	Yes
□	Does the solution provide a **definitive (as opposed to probabilistic or presumed)** answer as to whether the person on the other end of a call is a legitimate caller?	Yes
□	Does the solution deliver the ability to eliminate false positives?	Yes
□	Is the solution impervious to 1st caller fraud?*	Yes
□	Does the solution include direct carrier integration?	Yes
□	Does the solution include sophisticated SIP invite analysis?	Yes
□	Does the solution meet NIST AAL3 (highest level of assurance)?	Yes

Exhibit 12 at 1.



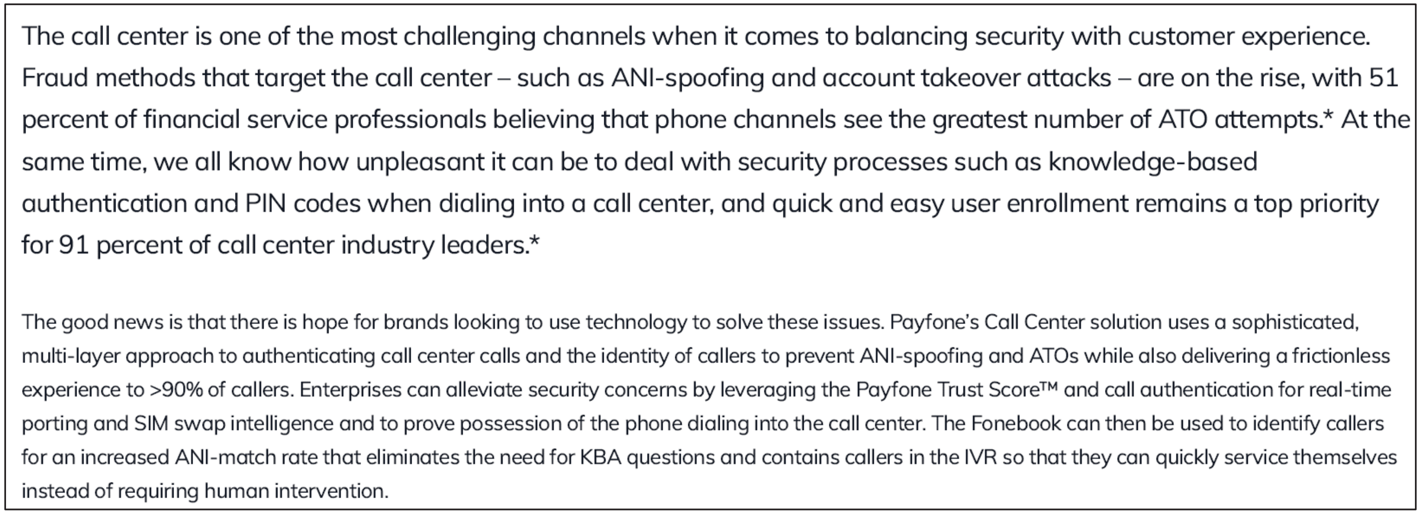
Trust Score

The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.)

In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust.

The Trust Score lets businesses confidently service customers and promote new offers.

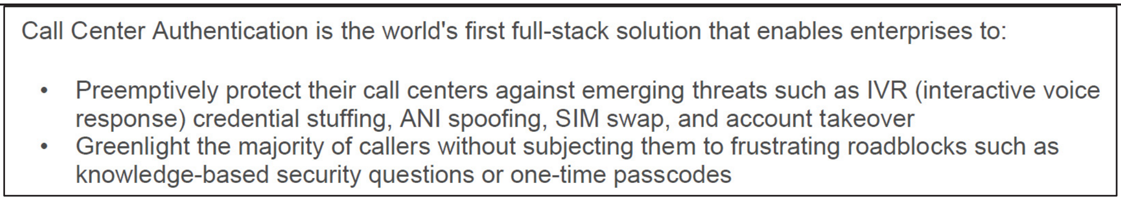
Exhibit 17 at 3.



The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.*

The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention.

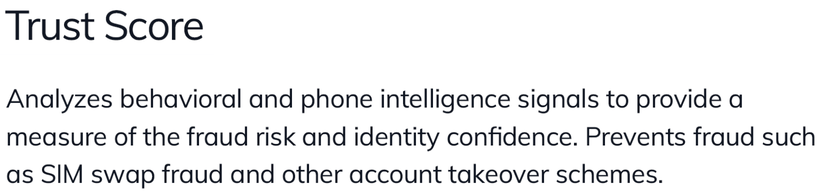
Exhibit 10 at 1.



Call Center Authentication is the world's first full-stack solution that enables enterprises to:

- Preemptively protect their call centers against emerging threats such as IVR (interactive voice response) credential stuffing, ANI spoofing, SIM swap, and account takeover
- Greenlight the majority of callers without subjecting them to frustrating roadblocks such as knowledge-based security questions or one-time passcodes

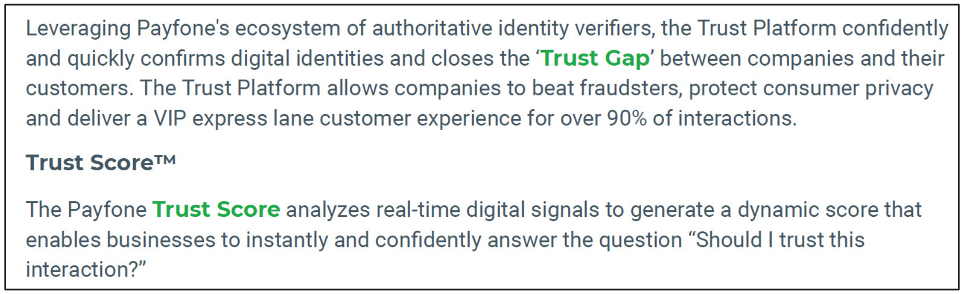
Exhibit 9 at 2.



Trust Score

Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes.

Exhibit 8 at 1-2.

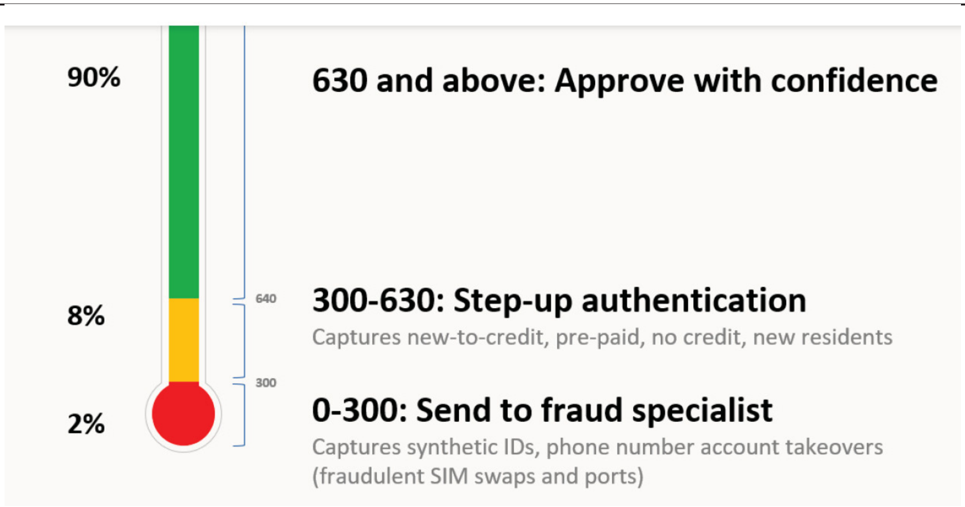
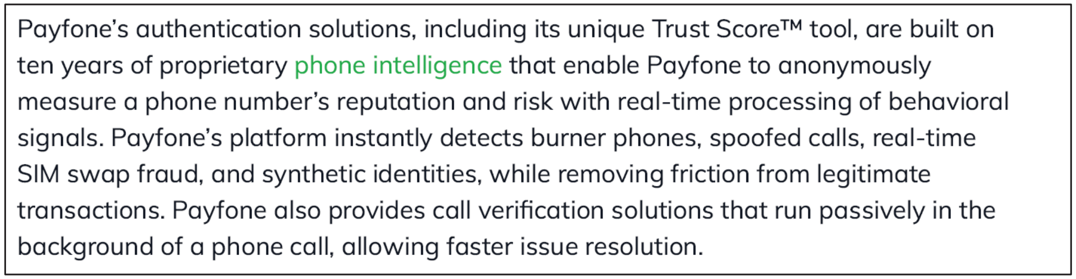


Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the '**Trust Gap**' between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions.

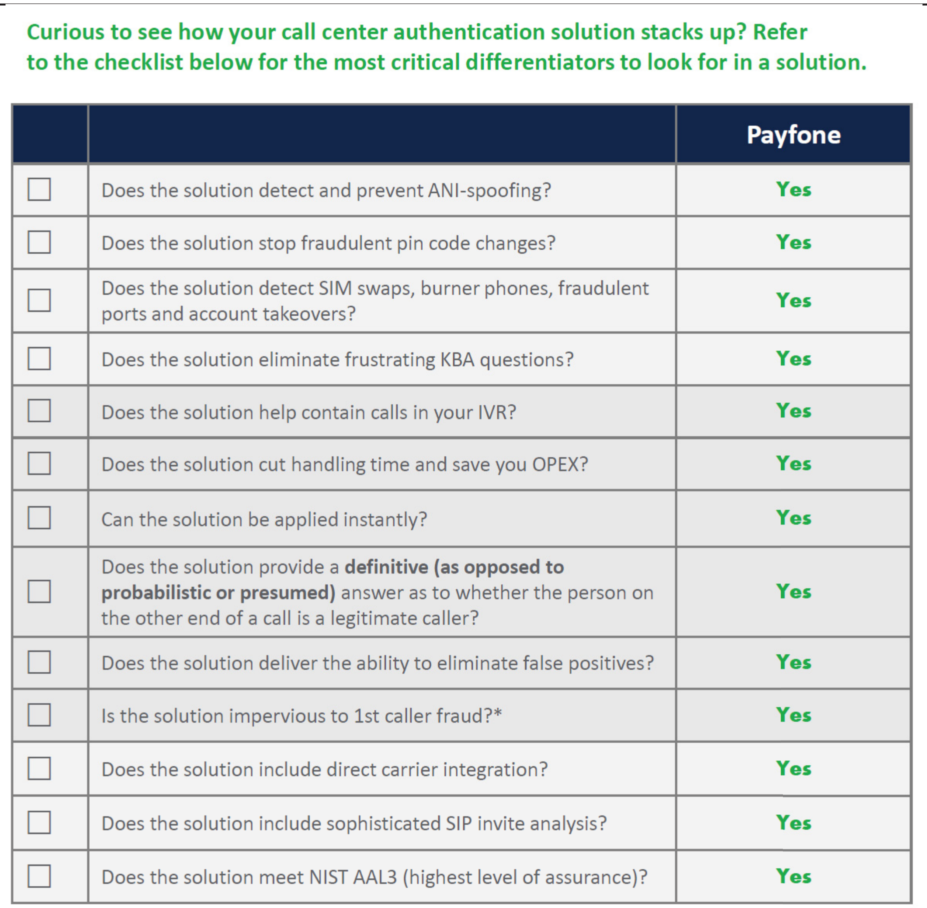
Trust Score™

The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question "Should I trust this interaction?"

Exhibit 11 at 4.

	 **630 and above: Approve with confidence** **300-630: Step-up authentication** Captures new-to-credit, pre-paid, no credit, new residents **0-300: Send to fraud specialist** Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports) *Exhibit 11 at 5.*  Payfone's authentication solutions, including its unique Trust Score™ tool, are built on ten years of proprietary phone intelligence that enable Payfone to anonymously measure a phone number's reputation and risk with real-time processing of behavioral signals. Payfone's platform instantly detects burner phones, spoofed calls, real-time SIM swap fraud, and synthetic identities, while removing friction from legitimate transactions. Payfone also provides call verification solutions that run passively in the background of a phone call, allowing faster issue resolution. *Exhibit 15 at 2.*
determining whether the number of accounts is between one and a threshold value, inclusive;	On information and belief, Prove's Call Center Authentication determines whether the number of accounts is between one and a threshold value.

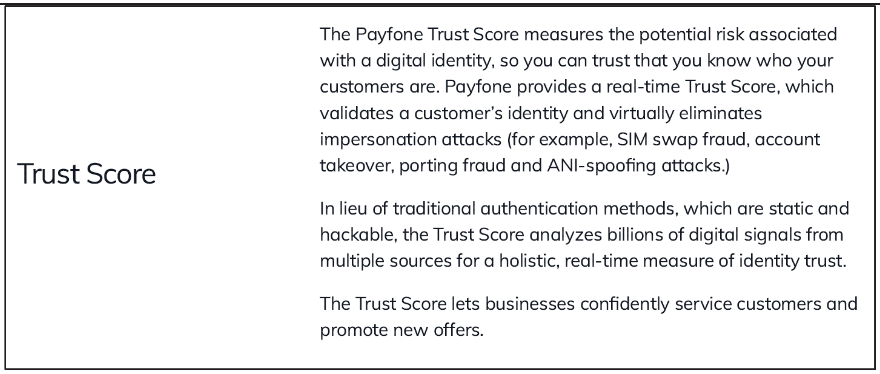
PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT



Curious to see how your call center authentication solution stacks up? Refer to the checklist below for the most critical differentiators to look for in a solution.

		Payfone
□	Does the solution detect and prevent ANI-spoofing?	Yes
□	Does the solution stop fraudulent pin code changes?	Yes
□	Does the solution detect SIM swaps, burner phones, fraudulent ports and account takeovers?	Yes
□	Does the solution eliminate frustrating KBA questions?	Yes
□	Does the solution help contain calls in your IVR?	Yes
□	Does the solution cut handling time and save you OPEX?	Yes
□	Can the solution be applied instantly?	Yes
□	Does the solution provide a **definitive (as opposed to probabilistic or presumed)** answer as to whether the person on the other end of a call is a legitimate caller?	Yes
□	Does the solution deliver the ability to eliminate false positives?	Yes
□	Is the solution impervious to 1st caller fraud?*	Yes
□	Does the solution include direct carrier integration?	Yes
□	Does the solution include sophisticated SIP invite analysis?	Yes
□	Does the solution meet NIST AAL3 (highest level of assurance)?	Yes

Exhibit 12 at 1.



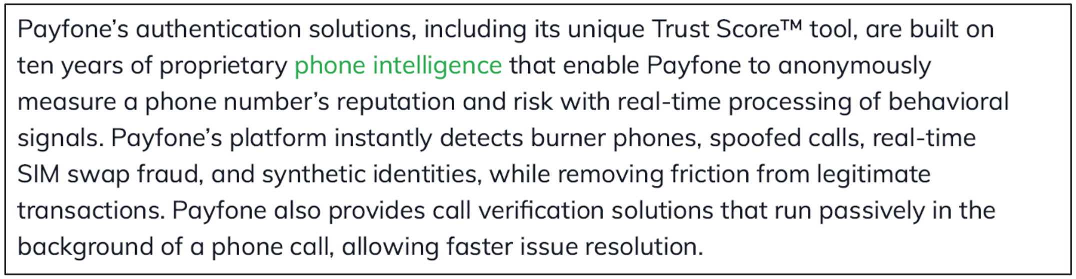
Trust Score

The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.)

In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust.

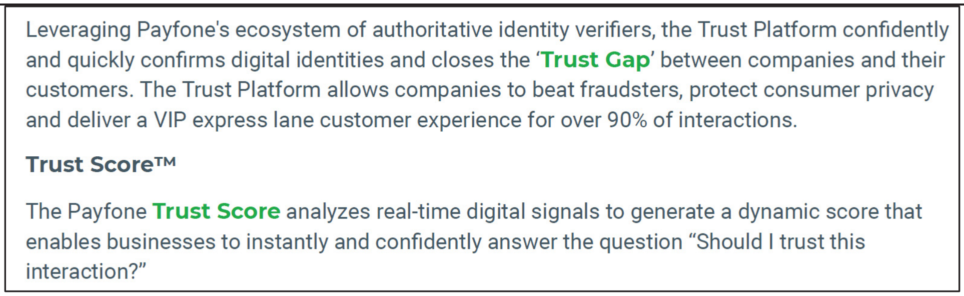
The Trust Score lets businesses confidently service customers and promote new offers.

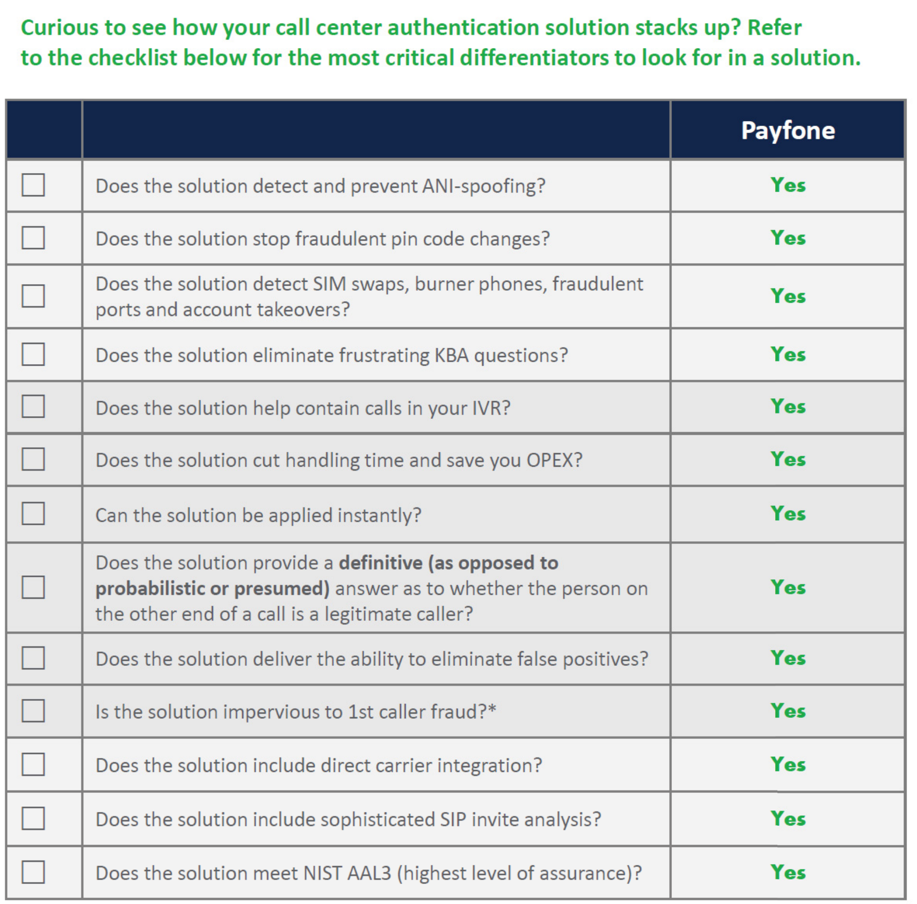
Exhibit 17 at 3.



Payfone's authentication solutions, including its unique Trust Score™ tool, are built on ten years of proprietary phone intelligence that enable Payfone to anonymously measure a phone number's reputation and risk with real-time processing of behavioral signals. Payfone's platform instantly detects burner phones, spoofed calls, real-time SIM swap fraud, and synthetic identities, while removing friction from legitimate transactions. Payfone also provides call verification solutions that run passively in the background of a phone call, allowing faster issue resolution.

Exhibit 15 at 2

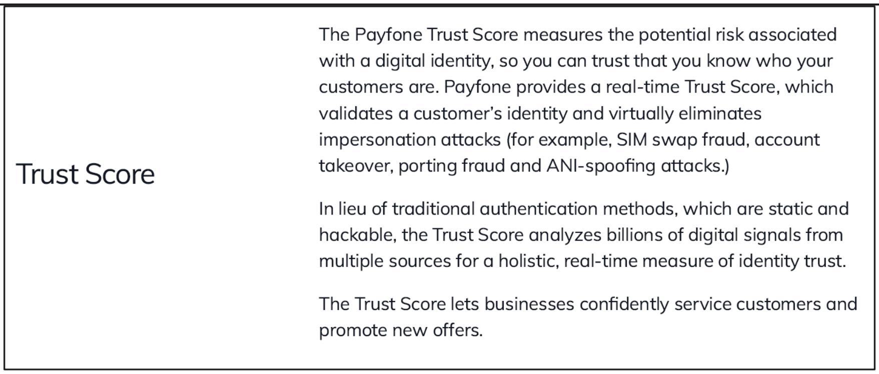
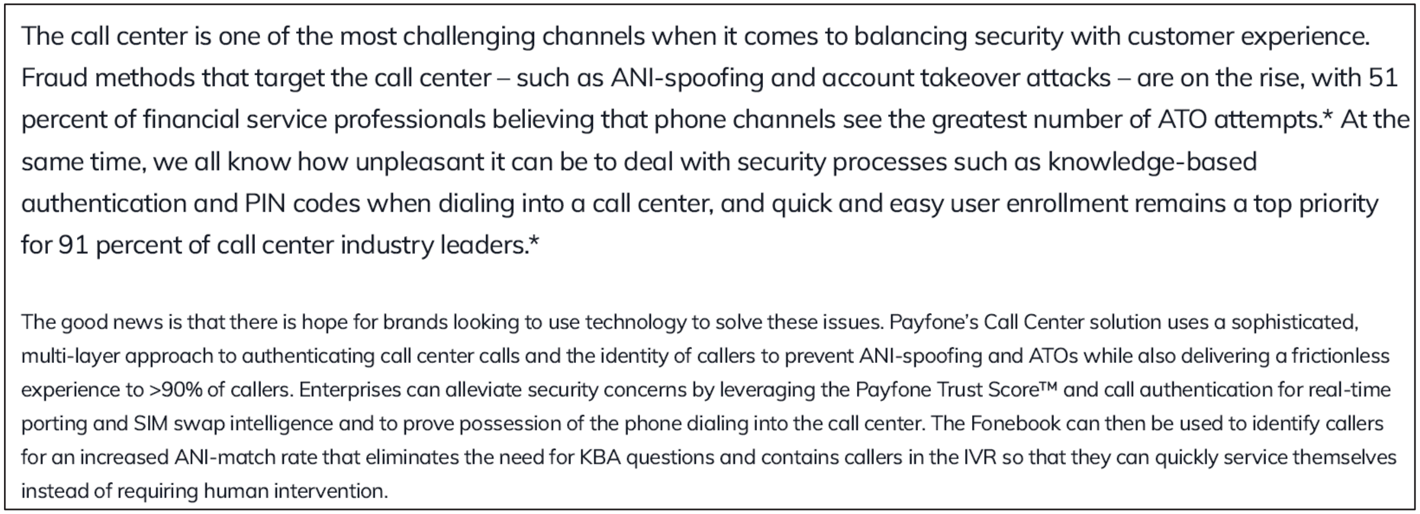
	 Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the '**Trust Gap**' between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions. **Trust Score™** The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question "Should I trust this interaction?" *Exhibit 11 at 4.*
authenticating, by the authentication device, the calling party number by verifying that the call request originates from a location or a device associated with the calling party number;	On information and belief, Prove's Call Center Authentication authenticates the calling party number by verifying that the call request originates from a location or a device associated with the calling party number (e.g., by generating a Trust Score).

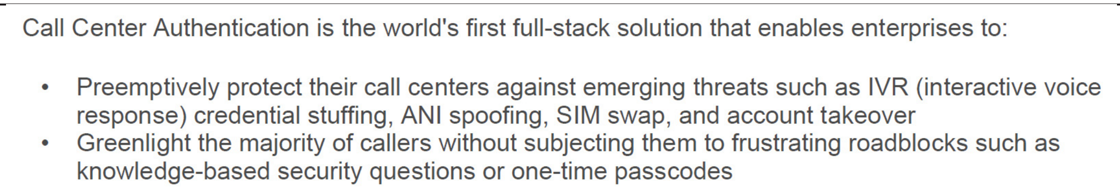


Curious to see how your call center authentication solution stacks up? Refer to the checklist below for the most critical differentiators to look for in a solution.

		Payfone
□	Does the solution detect and prevent ANI-spoofing?	**Yes**
□	Does the solution stop fraudulent pin code changes?	**Yes**
□	Does the solution detect SIM swaps, burner phones, fraudulent ports and account takeovers?	**Yes**
□	Does the solution eliminate frustrating KBA questions?	**Yes**
□	Does the solution help contain calls in your IVR?	**Yes**
□	Does the solution cut handling time and save you OPEX?	**Yes**
□	Can the solution be applied instantly?	**Yes**
□	Does the solution provide a **definitive (as opposed to probabilistic or presumed)** answer as to whether the person on the other end of a call is a legitimate caller?	**Yes**
□	Does the solution deliver the ability to eliminate false positives?	**Yes**
□	Is the solution impervious to 1st caller fraud?*	**Yes**
□	Does the solution include direct carrier integration?	**Yes**
□	Does the solution include sophisticated SIP invite analysis?	**Yes**
□	Does the solution meet NIST AAL3 (highest level of assurance)?	**Yes**

Exhibit 12 at 1.

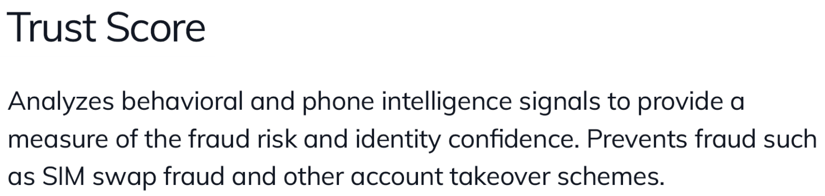
	 Trust Score The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.) In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust. The Trust Score lets businesses confidently service customers and promote new offers. *Exhibit 17 at 3.*  The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.* The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention. *Exhibit 10 at 1.*



Call Center Authentication is the world's first full-stack solution that enables enterprises to:

- Preemptively protect their call centers against emerging threats such as IVR (interactive voice response) credential stuffing, ANI spoofing, SIM swap, and account takeover
- Greenlight the majority of callers without subjecting them to frustrating roadblocks such as knowledge-based security questions or one-time passcodes

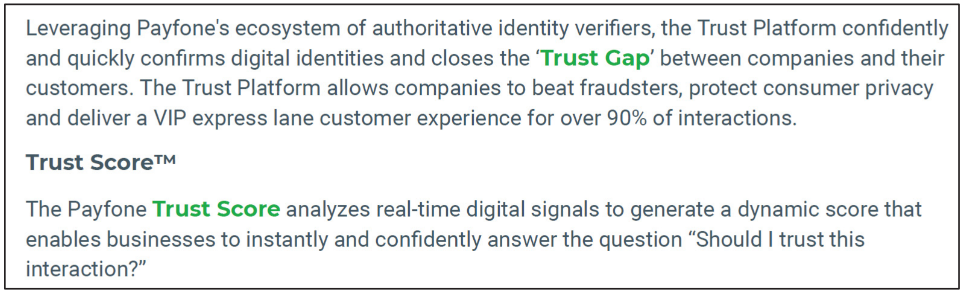
Exhibit 9 at 2.



Trust Score

Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes.

Exhibit 8 at 1-2.

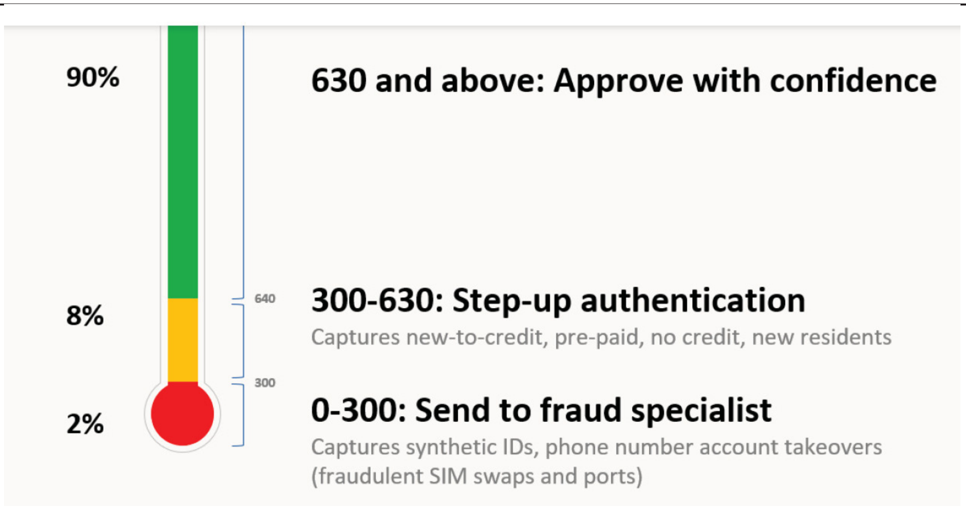
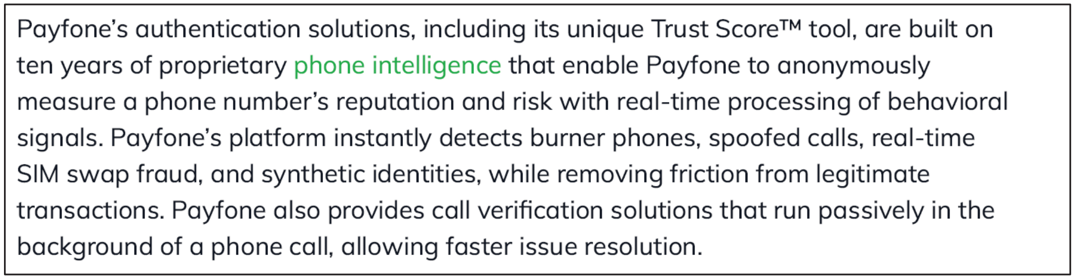


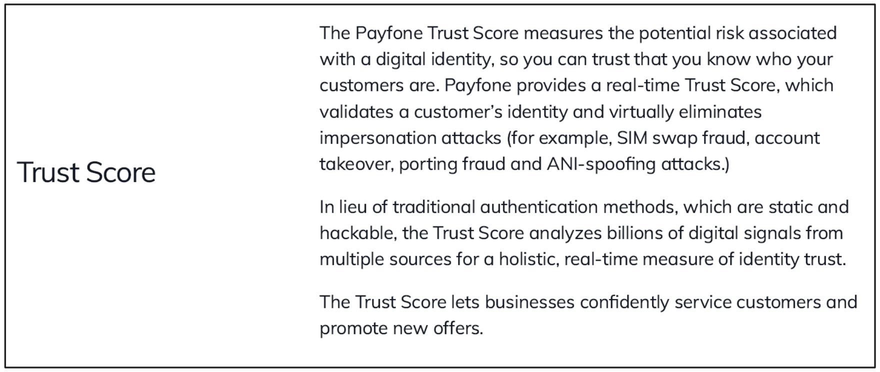
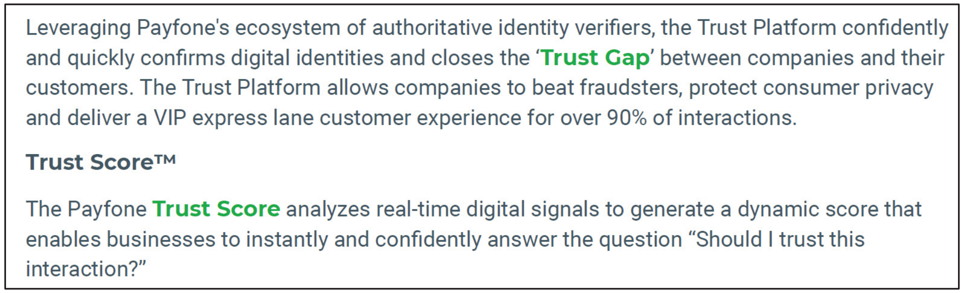
Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the '**Trust Gap**' between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions.

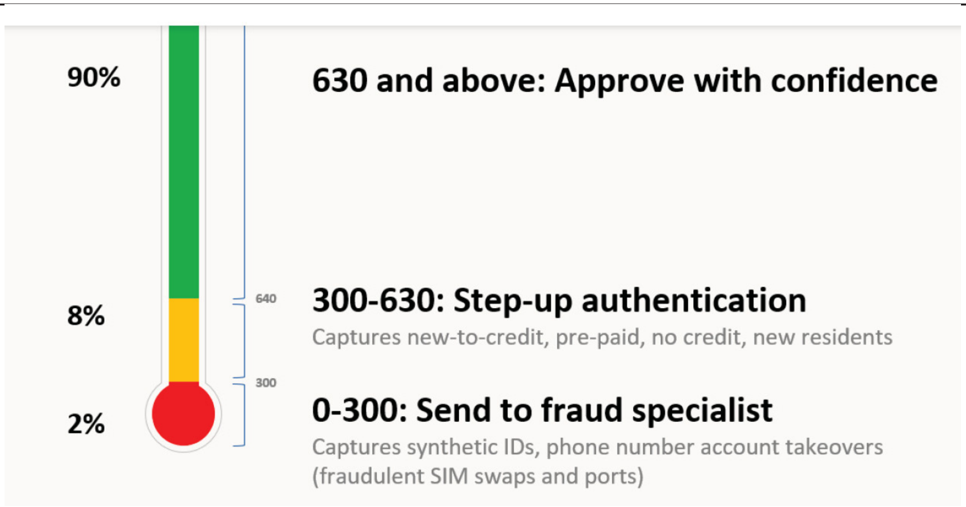
Trust Score™

The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question "Should I trust this interaction?"

Exhibit 11 at 4.

	 **630 and above: Approve with confidence** **300-630: Step-up authentication** Captures new-to-credit, pre-paid, no credit, new residents **0-300: Send to fraud specialist** Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports) *Exhibit 11 at 5.*  Payfone's authentication solutions, including its unique Trust Score™ tool, are built on ten years of proprietary phone intelligence that enable Payfone to anonymously measure a phone number's reputation and risk with real-time processing of behavioral signals. Payfone's platform instantly detects burner phones, spoofed calls, real-time SIM swap fraud, and synthetic identities, while removing friction from legitimate transactions. Payfone also provides call verification solutions that run passively in the background of a phone call, allowing faster issue resolution. *Exhibit 15 at 2.*
generating, by the authentication device based on the verifying and whether the number of accounts is determined to be between one and the threshold	On information and belief, Prove's Call Center Authentication generates, based on the verifying and whether the number of accounts is determined to be between one and the threshold value, an authentication result (e.g., Trust Score) indicating whether the calling party

value, an authentication result indicating whether the calling party number is authenticated; and	number is authenticated.  Trust Score The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.) In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust. The Trust Score lets businesses confidently service customers and promote new offers. *Exhibit 17 at 3.*  Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the '**Trust Gap**' between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions. **Trust Score™** The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question "Should I trust this interaction?" *Exhibit 11 at 4.*



630 and above: Approve with confidence

300-630: Step-up authentication
Captures new-to-credit, pre-paid, no credit, new residents

0-300: Send to fraud specialist
Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports)

Exhibit 11 at 5.

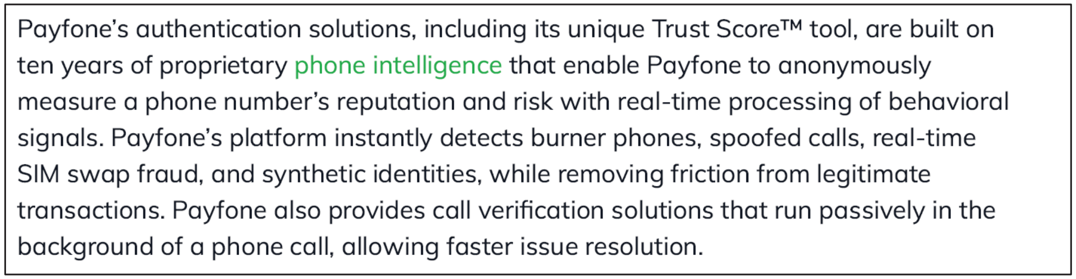
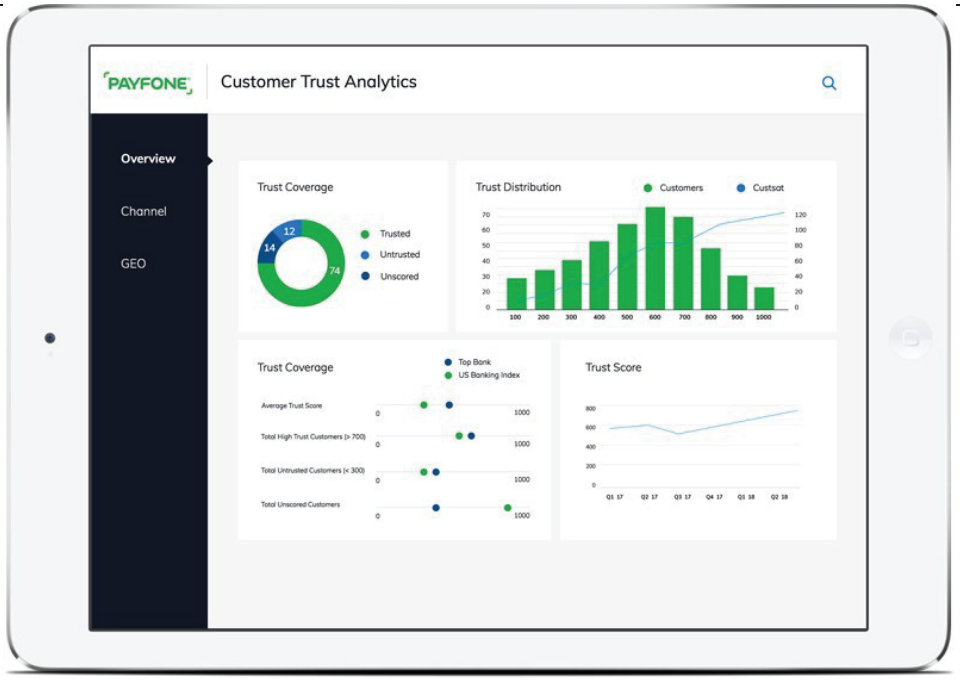
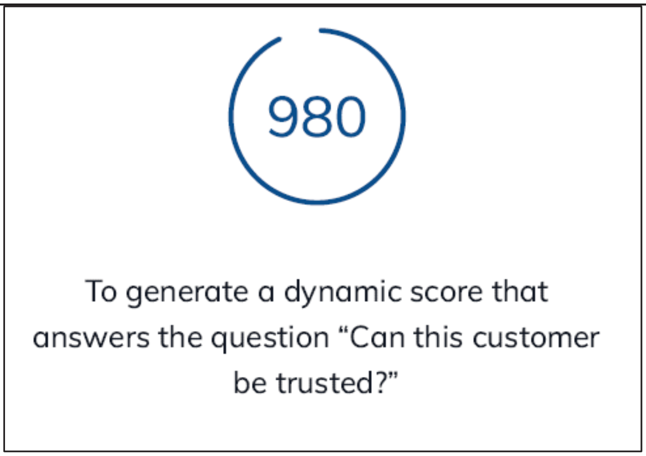
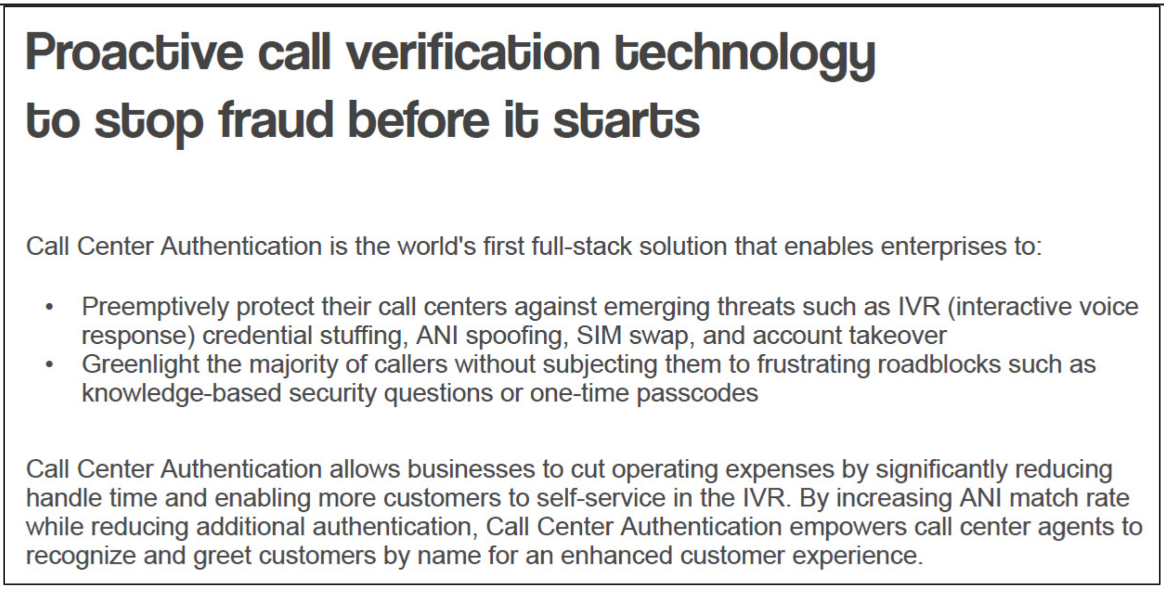
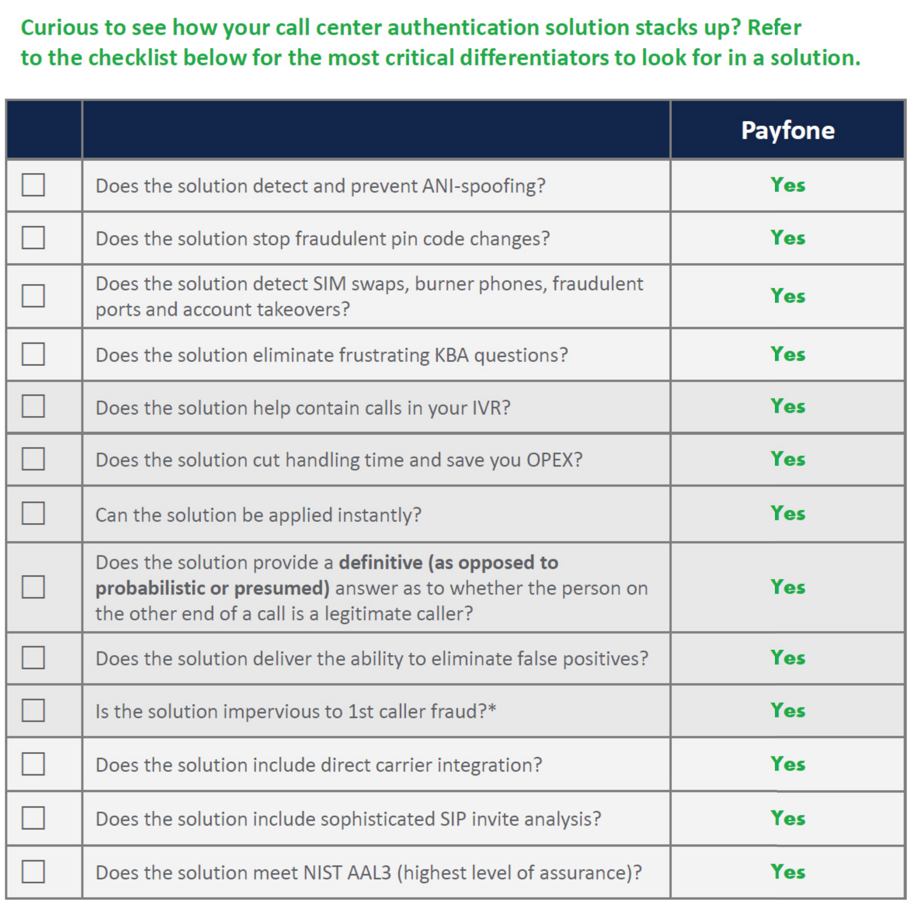

Payfone's authentication solutions, including its unique Trust Score™ tool, are built on ten years of proprietary phone intelligence that enable Payfone to anonymously measure a phone number's reputation and risk with real-time processing of behavioral signals. Payfone's platform instantly detects burner phones, spoofed calls, real-time SIM swap fraud, and synthetic identities, while removing friction from legitimate transactions. Payfone also provides call verification solutions that run passively in the background of a phone call, allowing faster issue resolution.

Exhibit 15 at 2.

	 PAYFONE Customer Trust Analytics Overview Channel GEO Trust Coverage 12 14 74 ● Trusted ● Untrusted ● Unscored Trust Distribution ● Customers ● Custsat 70 60 50 40 30 20 0 120 100 80 60 40 20 0 100 200 300 400 500 600 700 800 900 1000 Trust Coverage ● Top Bank ● US Banking Index Average Trust Score Total High Trust Customers (> 700) Total Untrusted Customers (< 300) Total Unscored Customers 0 1000 Trust Score 800 600 400 200 0 Q1 17 Q2 17 Q3 17 Q4 17 Q1 18 Q2 18 *Exhibit 20 at 1.*

	 To generate a dynamic score that answers the question "Can this customer be trusted?" *Exhibit 17 at 3.*
sending, by the authentication device, the authentication result to a call processing device that processes the call request from the caller according to the authentication result.	On information and belief, Prove's Call Center Authentication sends the authentication result (e.g., Trust Score) to a call processing device that processes the call request from the caller according to the authentication result.

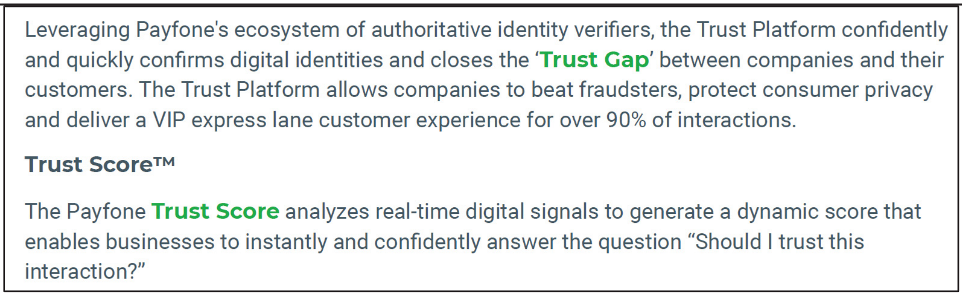
	 **Proactive call verification technology to stop fraud before it starts** Call Center Authentication is the world's first full-stack solution that enables enterprises to: • Preemptively protect their call centers against emerging threats such as IVR (interactive voice response) credential stuffing, ANI spoofing, SIM swap, and account takeover • Greenlight the majority of callers without subjecting them to frustrating roadblocks such as knowledge-based security questions or one-time passcodes Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience. *Exhibit 9 at 2.*



Curious to see how your call center authentication solution stacks up? Refer to the checklist below for the most critical differentiators to look for in a solution.

		Payfone
□	Does the solution detect and prevent ANI-spoofing?	**Yes**
□	Does the solution stop fraudulent pin code changes?	**Yes**
□	Does the solution detect SIM swaps, burner phones, fraudulent ports and account takeovers?	**Yes**
□	Does the solution eliminate frustrating KBA questions?	**Yes**
□	Does the solution help contain calls in your IVR?	**Yes**
□	Does the solution cut handling time and save you OPEX?	**Yes**
□	Can the solution be applied instantly?	**Yes**
□	Does the solution provide a **definitive (as opposed to probabilistic or presumed)** answer as to whether the person on the other end of a call is a legitimate caller?	**Yes**
□	Does the solution deliver the ability to eliminate false positives?	**Yes**
□	Is the solution impervious to 1st caller fraud?*	**Yes**
□	Does the solution include direct carrier integration?	**Yes**
□	Does the solution include sophisticated SIP invite analysis?	**Yes**
□	Does the solution meet NIST AAL3 (highest level of assurance)?	**Yes**

Exhibit 12 at 1.

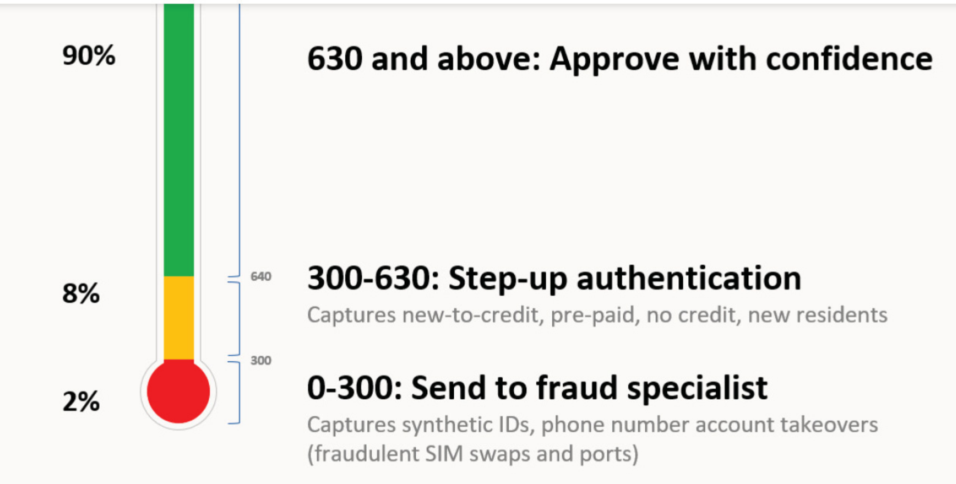


Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the '**Trust Gap**' between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions.

Trust Score™

The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question "Should I trust this interaction?"

Exhibit 11 at 4.



630 and above: Approve with confidence

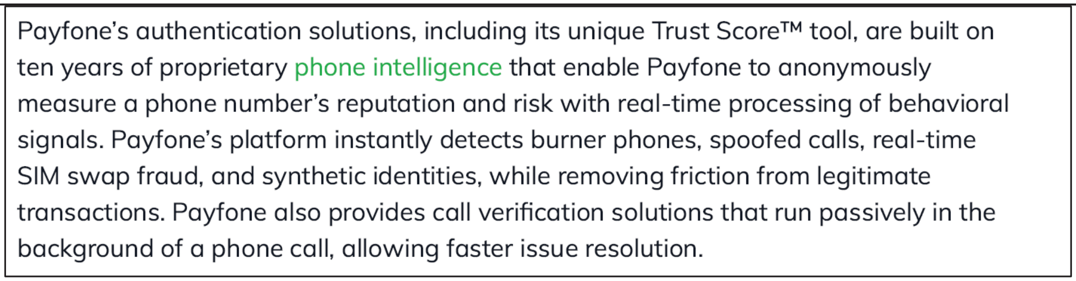
300-630: Step-up authentication

Captures new-to-credit, pre-paid, no credit, new residents

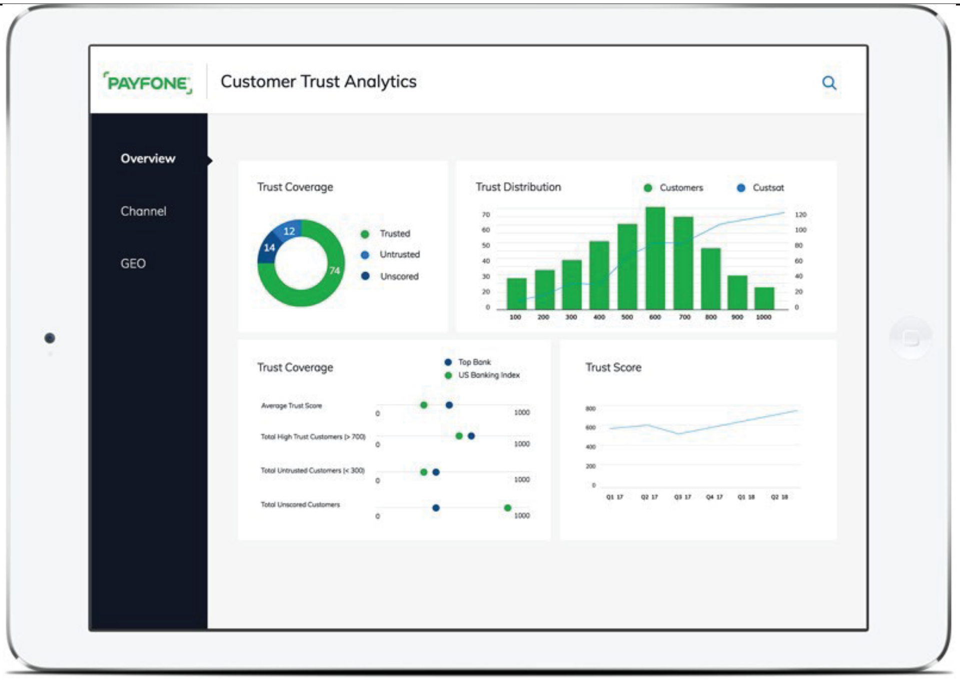
0-300: Send to fraud specialist

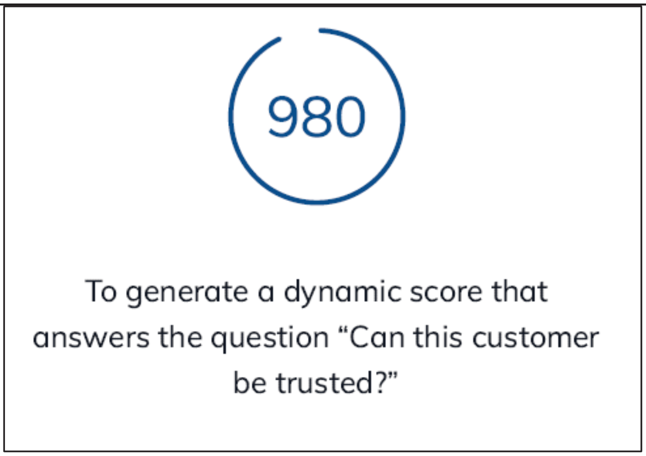
Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports)

Exhibit 11 at 5.

	 Payfone's authentication solutions, including its unique Trust Score™ tool, are built on ten years of proprietary phone intelligence that enable Payfone to anonymously measure a phone number's reputation and risk with real-time processing of behavioral signals. Payfone's platform instantly detects burner phones, spoofed calls, real-time SIM swap fraud, and synthetic identities, while removing friction from legitimate transactions. Payfone also provides call verification solutions that run passively in the background of a phone call, allowing faster issue resolution. *Exhibit 15 at 2.*

**PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT**

	 PAYFONE Customer Trust Analytics Overview Channel GEO Trust Coverage 12 14 74 Trusted Untrusted Unscored Trust Distribution Customers Custsat 70 60 50 40 30 20 0 120 100 80 60 40 20 0 100 200 300 400 500 600 700 800 900 1000 Trust Coverage Top Bank US Banking Index Average Trust Score Total High Trust Customers (> 700) Total Untrusted Customers (< 300) Total Unscored Customers 0 1000 Trust Score 800 600 400 200 0 Q1 17 Q2 17 Q3 17 Q4 17 Q1 18 Q2 18 *Exhibit 20 at 1.*

	 To generate a dynamic score that answers the question “Can this customer be trusted?” *Exhibit 17 at 3.*

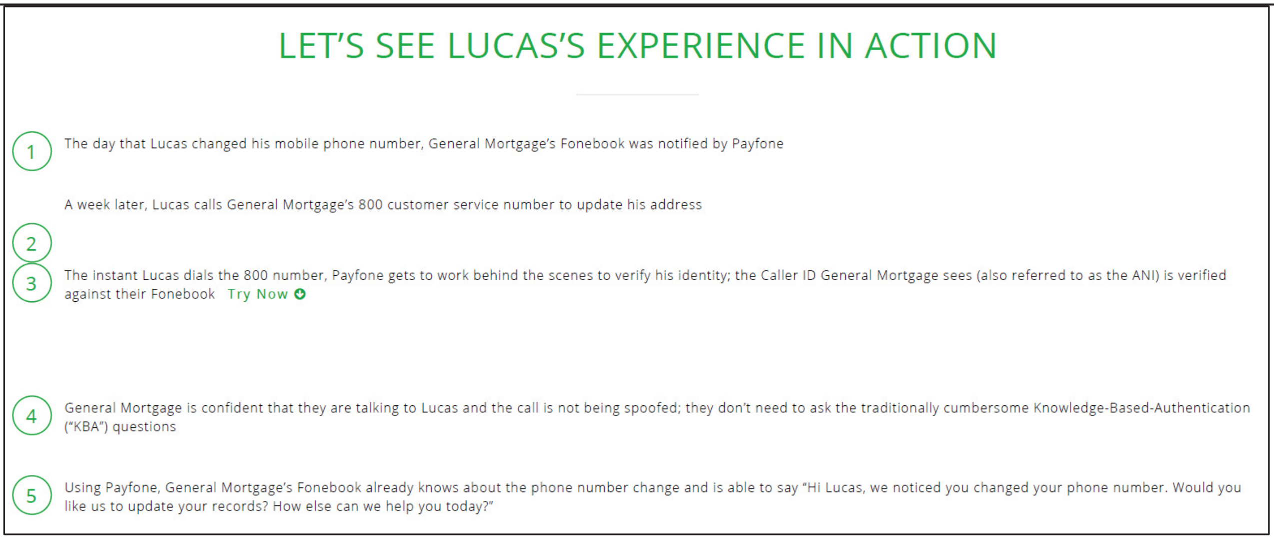
	 LET'S SEE LUCAS'S EXPERIENCE IN ACTION 1 The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone A week later, Lucas calls General Mortgage's 800 customer service number to update his address 2 3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now ⊕ 4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions 5 Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?" *Exhibit 13 at 1.*

Exhibit 26

US 10,693,840 Claim 1

Prove's Contact Identification

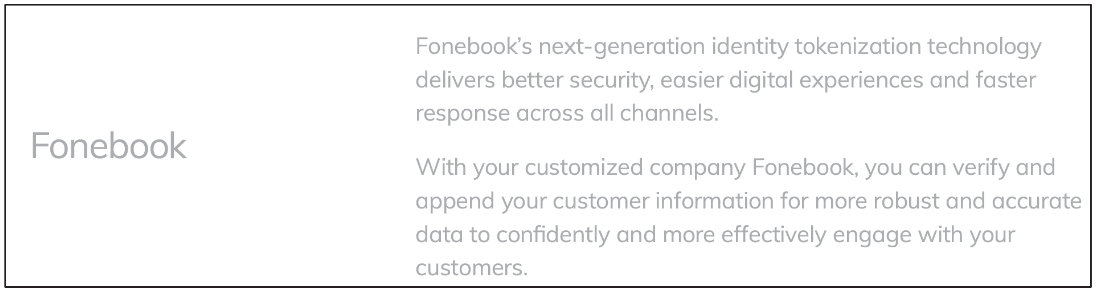
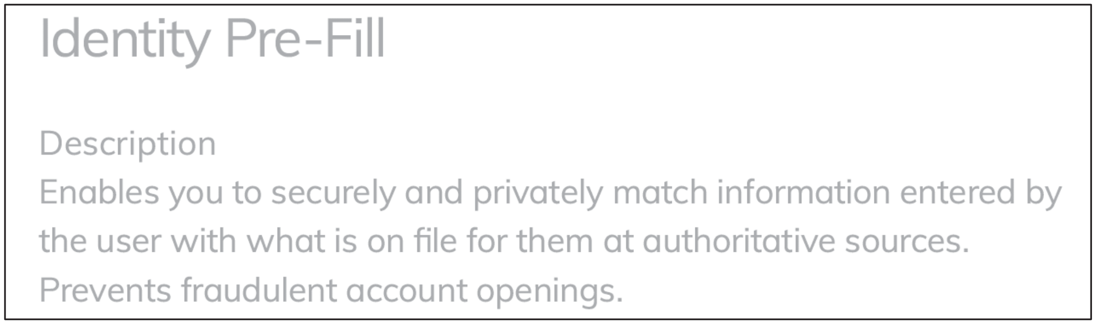
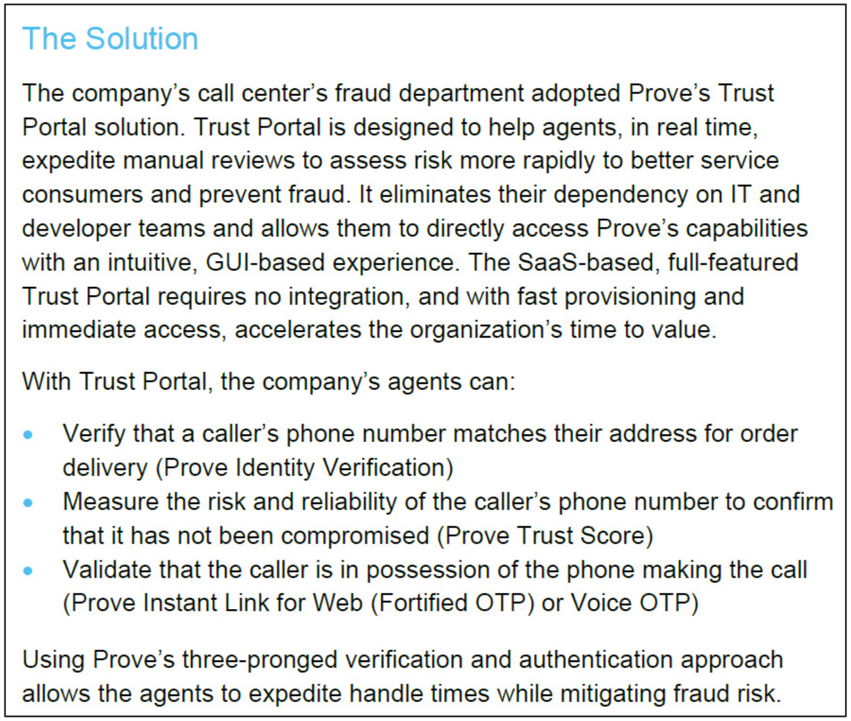
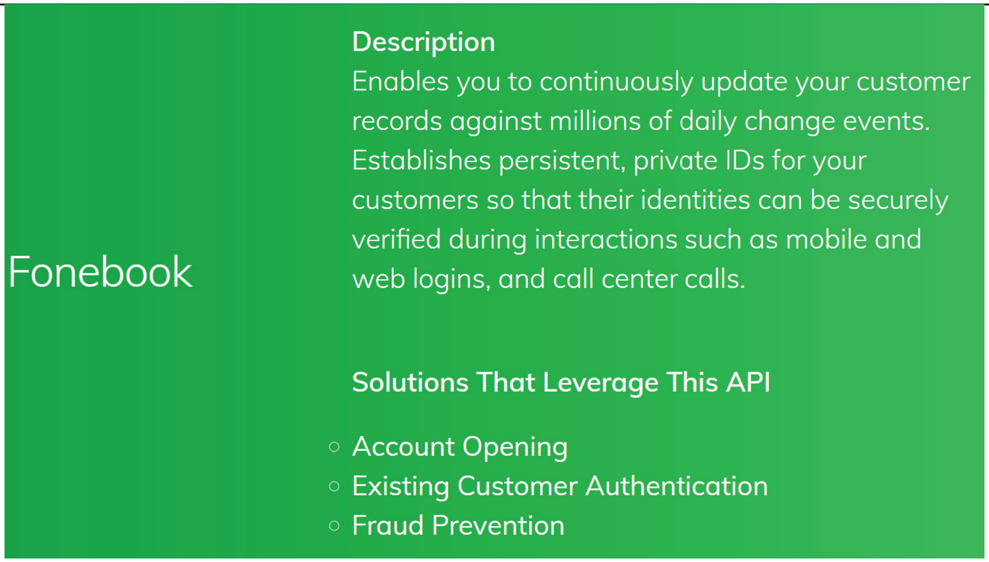
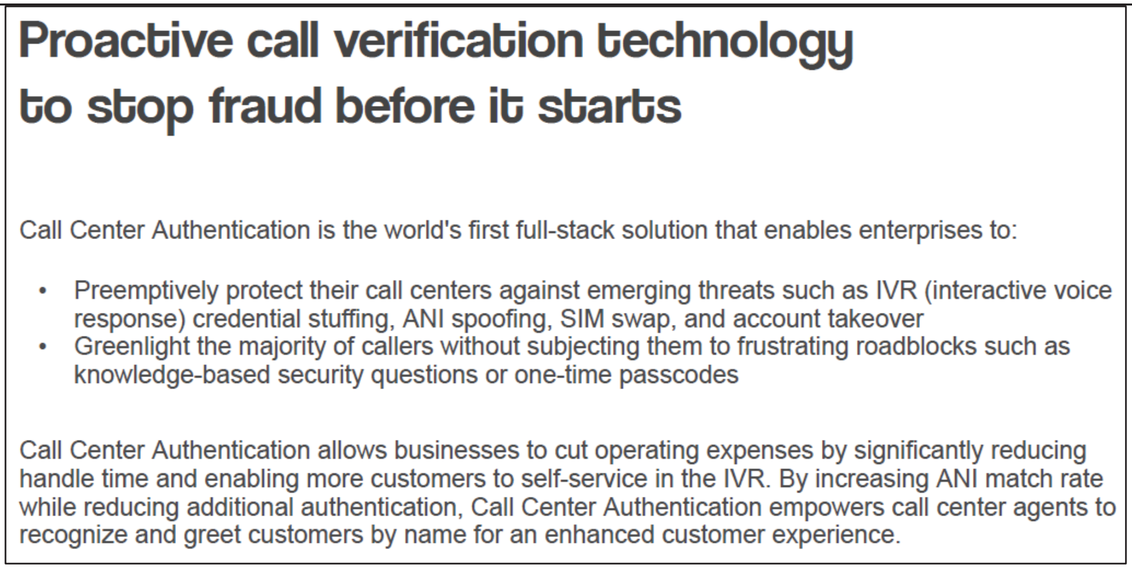
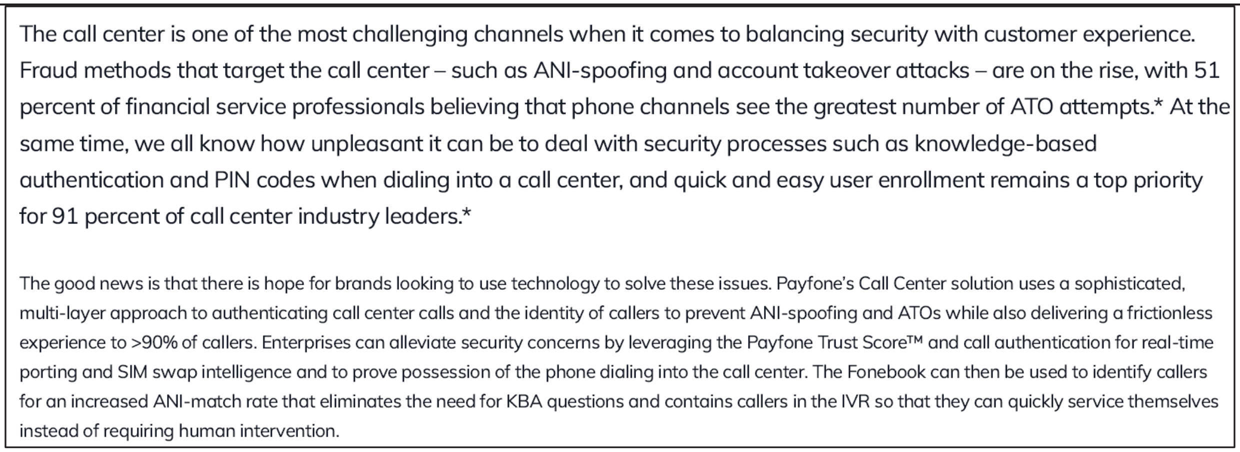
1. A method for sharing contact information of a first user between a first application and a second application associated with a second user, the method comprising using a server on a computer network to perform steps of:	On information and belief, Prove's Contact Identification includes a method for sharing contact information (e.g., Fonebook, Identity Pre-Fill) of a first user (e.g., caller) between a first application (e.g., database or telephony system) and a second application (e.g., IVR or CRM) associated with a second user (e.g., call center or agent), the method comprising using a server on a computer network.  Fonebook Fonebook's next-generation identity tokenization technology delivers better security, easier digital experiences and faster response across all channels. With your customized company Fonebook, you can verify and append your customer information for more robust and accurate data to confidently and more effectively engage with your customers. *Exhibit 17 at 2.*  Identity Pre-Fill Description Enables you to securely and privately match information entered by the user with what is on file for them at authoritative sources. Prevents fraudulent account openings.

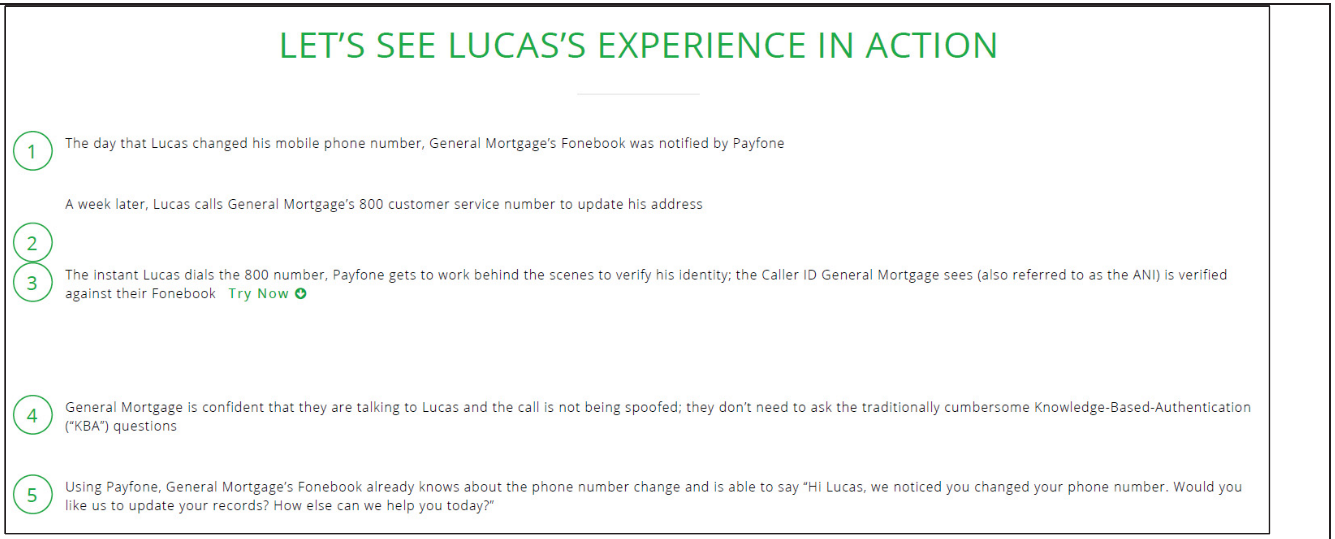
	Exhibit 8 at 3.  The Solution The company's call center's fraud department adopted Prove's Trust Portal solution. Trust Portal is designed to help agents, in real time, expedite manual reviews to assess risk more rapidly to better service consumers and prevent fraud. It eliminates their dependency on IT and developer teams and allows them to directly access Prove's capabilities with an intuitive, GUI-based experience. The SaaS-based, full-featured Trust Portal requires no integration, and with fast provisioning and immediate access, accelerates the organization's time to value. With Trust Portal, the company's agents can: • Verify that a caller's phone number matches their address for order delivery (Prove Identity Verification) • Measure the risk and reliability of the caller's phone number to confirm that it has not been compromised (Prove Trust Score) • Validate that the caller is in possession of the phone making the call (Prove Instant Link for Web (Fortified OTP) or Voice OTP) Using Prove's three-pronged verification and authentication approach allows the agents to expedite handle times while mitigating fraud risk. *Exhibit 18 at 2.*

**PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT**

	 Fonebook **Description** Enables you to continuously update your customer records against millions of daily change events. Establishes persistent, private IDs for your customers so that their identities can be securely verified during interactions such as mobile and web logins, and call center calls. **Solutions That Leverage This API** ○ Account Opening ○ Existing Customer Authentication ○ Fraud Prevention *Exhibit 8 at* 2.

	 **Proactive call verification technology to stop fraud before it starts** Call Center Authentication is the world's first full-stack solution that enables enterprises to: • Preemptively protect their call centers against emerging threats such as IVR (interactive voice response) credential stuffing, ANI spoofing, SIM swap, and account takeover • Greenlight the majority of callers without subjecting them to frustrating roadblocks such as knowledge-based security questions or one-time passcodes Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience. *Exhibit 9 at 2.*

	 The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.* The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention. *Exhibit 10 at 1.*



LET'S SEE LUCAS'S EXPERIENCE IN ACTION

1 The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone

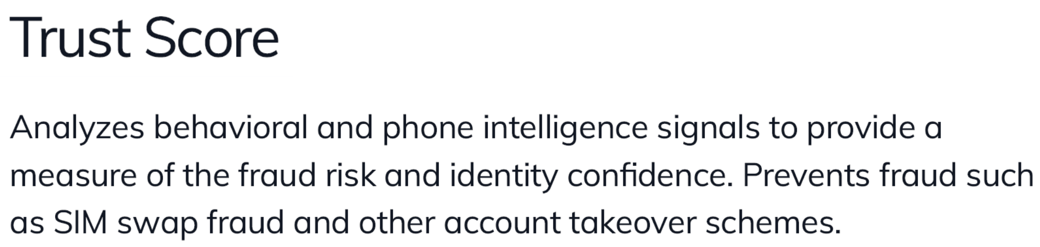
2 A week later, Lucas calls General Mortgage's 800 customer service number to update his address

3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now

4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions

5 Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?"

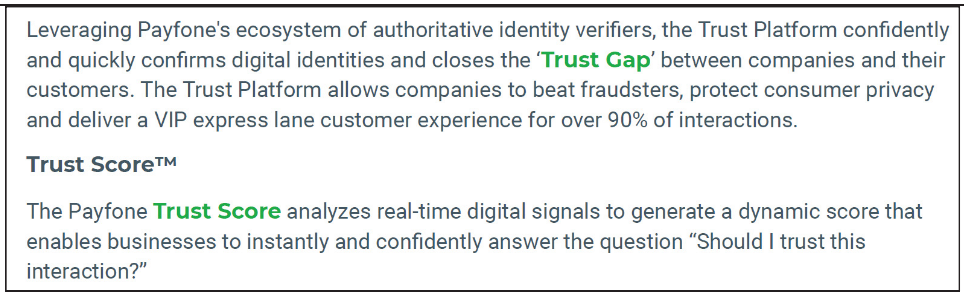
Exhibit 13 at 1.



Trust Score

Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes.

Exhibit 8 at 1-2.

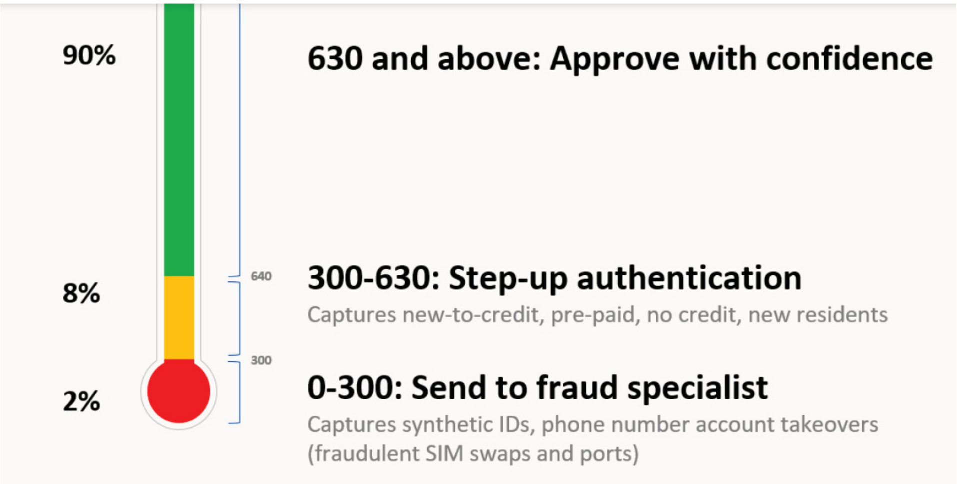


Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the '**Trust Gap**' between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions.

Trust Score™

The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question "Should I trust this interaction?"

Exhibit 11 at 4.



630 and above: Approve with confidence

300-630: Step-up authentication

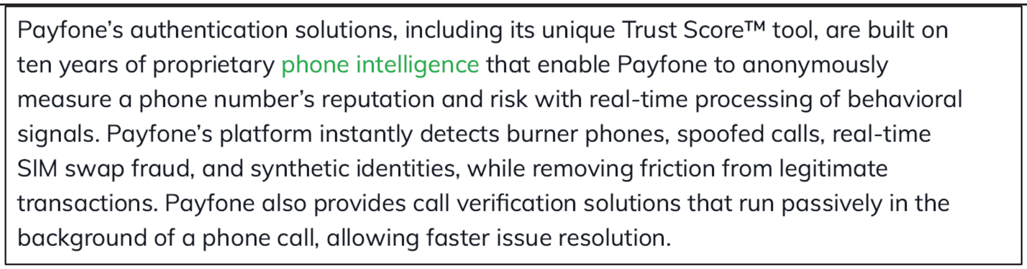
Captures new-to-credit, pre-paid, no credit, new residents

0-300: Send to fraud specialist

Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports)

Exhibit 11 at 5.

**PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT**



Payfone's authentication solutions, including its unique Trust Score™ tool, are built on ten years of proprietary phone intelligence that enable Payfone to anonymously measure a phone number's reputation and risk with real-time processing of behavioral signals. Payfone's platform instantly detects burner phones, spoofed calls, real-time SIM swap fraud, and synthetic identities, while removing friction from legitimate transactions. Payfone also provides call verification solutions that run passively in the background of a phone call, allowing faster issue resolution.

Exhibit 15 at 2.

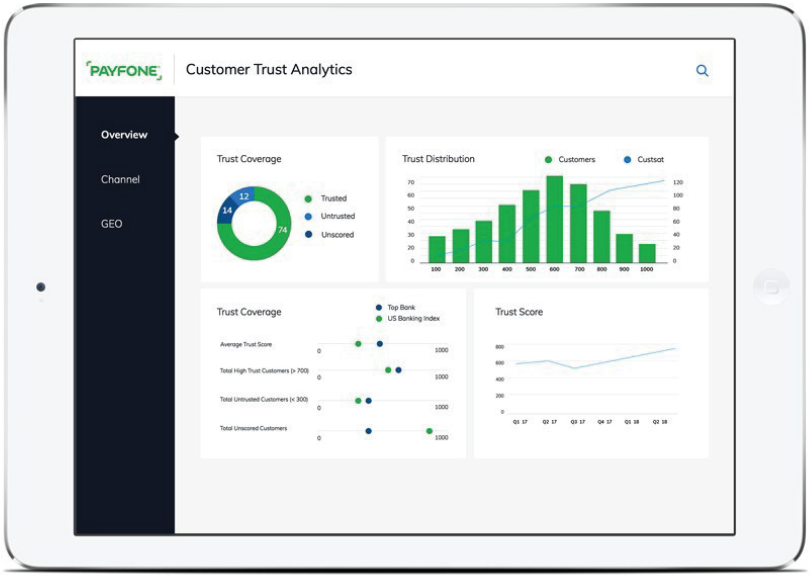
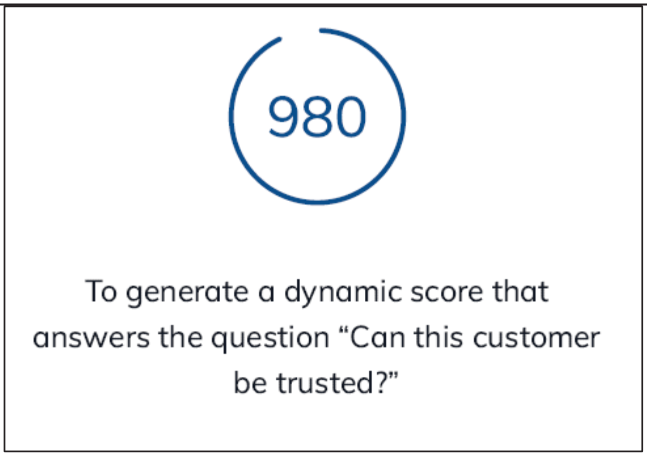
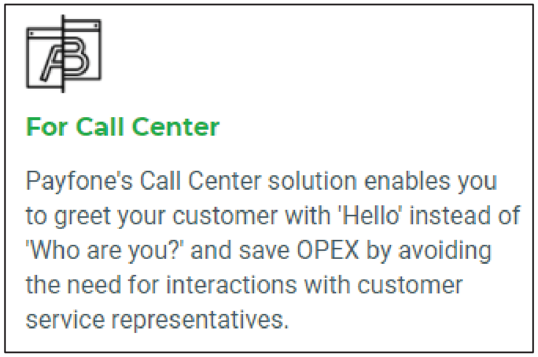
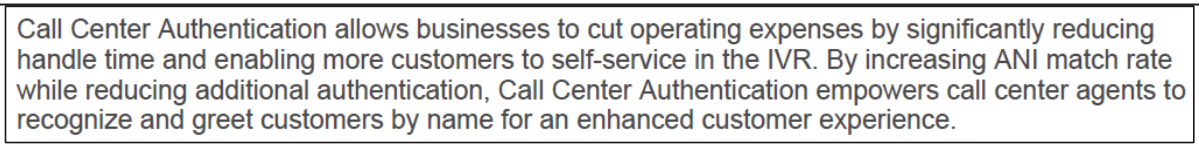
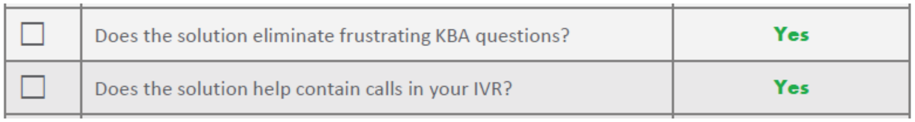
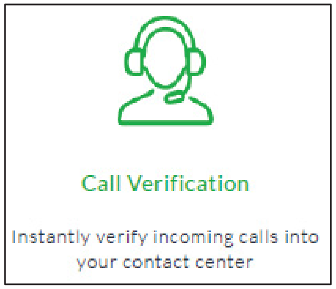
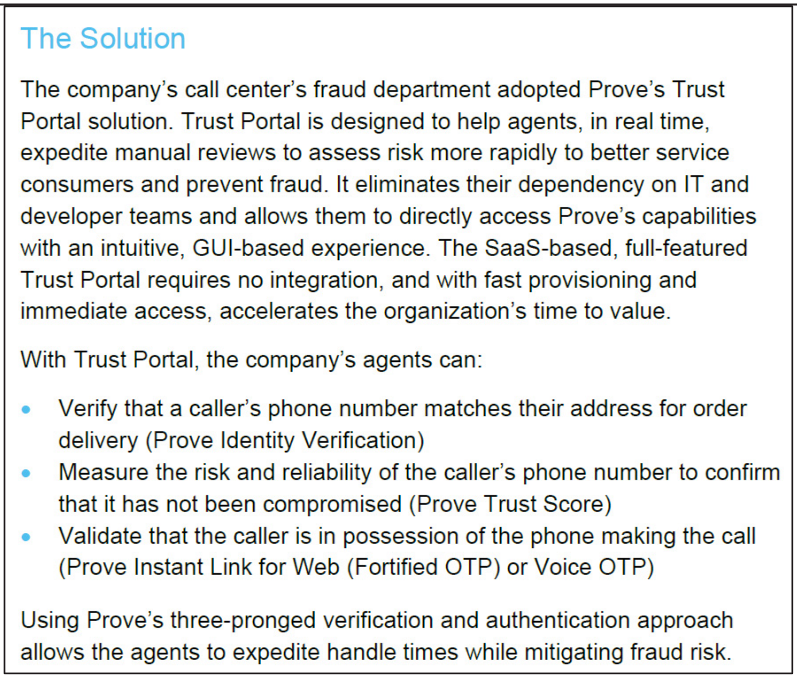


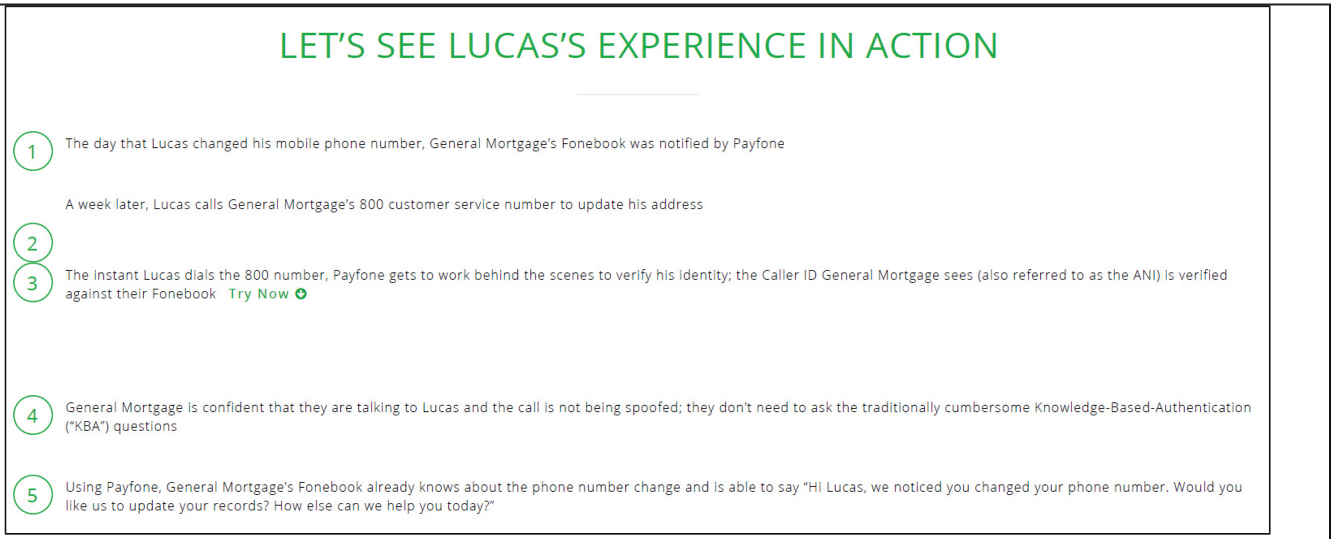
Exhibit 20 at 1.

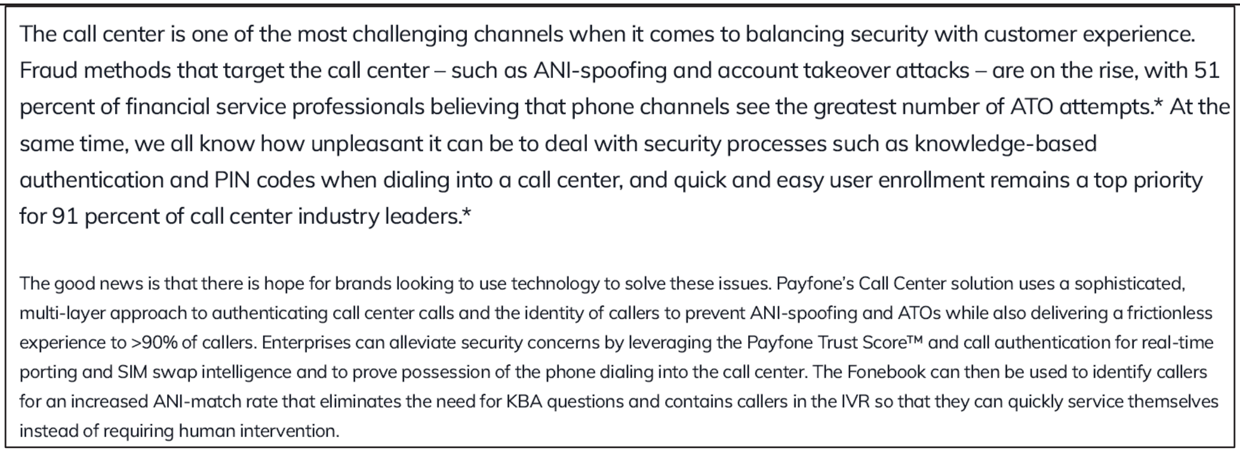
	 To generate a dynamic score that answers the question “Can this customer be trusted?” *Exhibit 17 at 3.*  **For Call Center** Payfone's Call Center solution enables you to greet your customer with 'Hello' instead of 'Who are you?' and save OPEX by avoiding the need for interactions with customer service representatives. *Exhibit 11 at 3.*

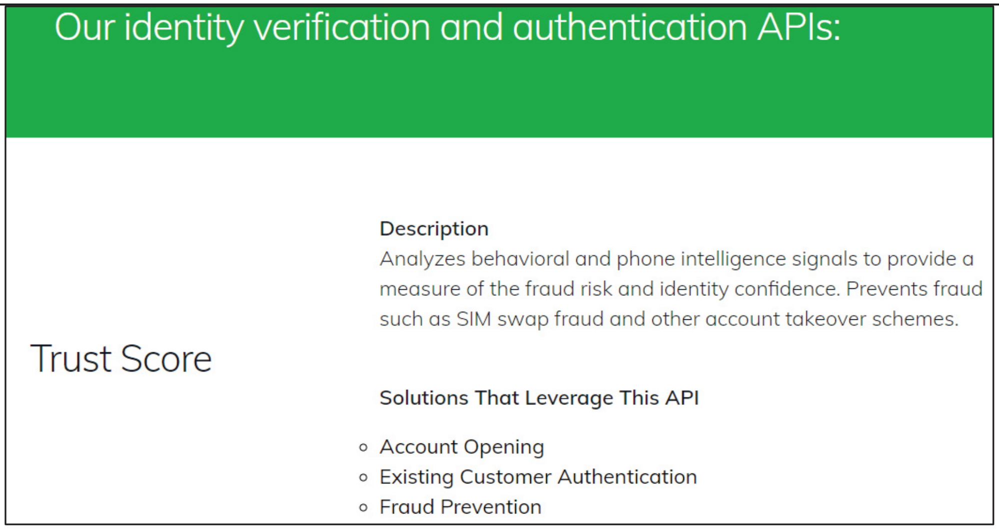
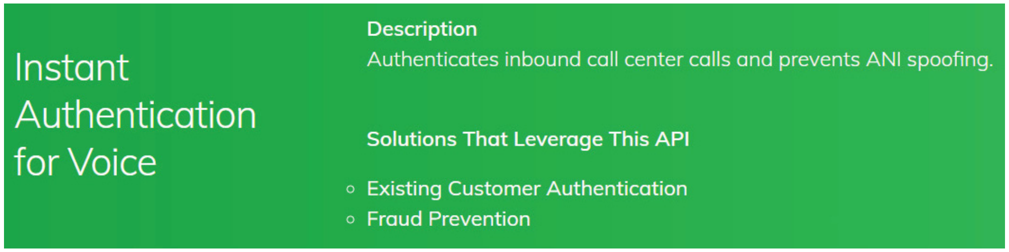
	 Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience. *Exhibit 9 at 2.*  ☐ Does the solution eliminate frustrating KBA questions? Yes ☐ Does the solution help contain calls in your IVR? Yes *Exhibit 12 at 1.*  Call Verification Instantly verify incoming calls into your contact center *Exhibit 21 at 1.*
identifying a first identifier relating to the first user;	On information and belief, Prove's Contact Identification identifies a first identifier (e.g., phone number or ANI) relating to the first user (e.g., caller).

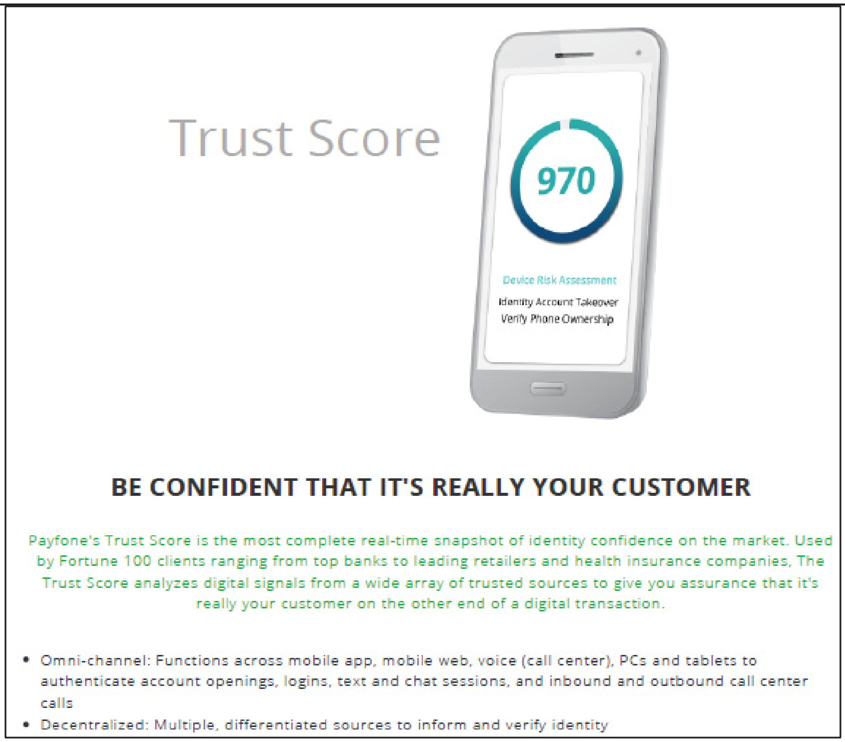
	 The Solution The company's call center's fraud department adopted Prove's Trust Portal solution. Trust Portal is designed to help agents, in real time, expedite manual reviews to assess risk more rapidly to better service consumers and prevent fraud. It eliminates their dependency on IT and developer teams and allows them to directly access Prove's capabilities with an intuitive, GUI-based experience. The SaaS-based, full-featured Trust Portal requires no integration, and with fast provisioning and immediate access, accelerates the organization's time to value. With Trust Portal, the company's agents can: • Verify that a caller's phone number matches their address for order delivery (Prove Identity Verification) • Measure the risk and reliability of the caller's phone number to confirm that it has not been compromised (Prove Trust Score) • Validate that the caller is in possession of the phone making the call (Prove Instant Link for Web (Fortified OTP) or Voice OTP) Using Prove's three-pronged verification and authentication approach allows the agents to expedite handle times while mitigating fraud risk. *Exhibit 18 at 2.*

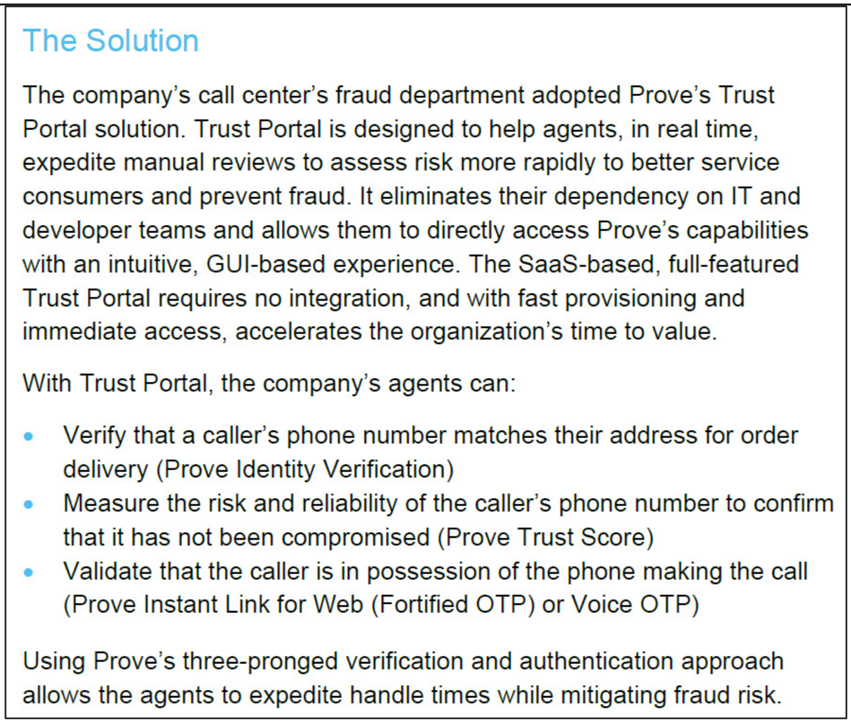
PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT

	 LET'S SEE LUCAS'S EXPERIENCE IN ACTION 1 The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone A week later, Lucas calls General Mortgage's 800 customer service number to update his address 2 3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now 4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions 5 Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?" *Exhibit 13 at 1.*

	 The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.* The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention. *Exhibit 10 at 1.*

	 Our identity verification and authentication APIs: Trust Score Description Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes. Solutions That Leverage This API ○ Account Opening ○ Existing Customer Authentication ○ Fraud Prevention *Exhibit 8 at 2.*  Instant Authentication for Voice Description Authenticates inbound call center calls and prevents ANI spoofing. Solutions That Leverage This API ○ Existing Customer Authentication ○ Fraud Prevention *Exhibit 8 at 4.*

	 970 Device Risk Assessment Identity Account Takeover Verify Phone Ownership Trust Score **BE CONFIDENT THAT IT'S REALLY YOUR CUSTOMER** Payfone's Trust Score is the most complete real-time snapshot of identity confidence on the market. Used by Fortune 100 clients ranging from top banks to leading retailers and health insurance companies. The Trust Score analyzes digital signals from a wide array of trusted sources to give you assurance that it's really your customer on the other end of a digital transaction. - Omni-channel: Functions across mobile app, mobile web, voice (call center), PCs and tablets to authenticate account openings, logins, text and chat sessions, and inbound and outbound call center calls - Decentralized: Multiple, differentiated sources to inform and verify identity *Exhibit 14 at 1.*
provisioning contact information associated with the first identifier, wherein the contact information includes a set of different identifiers, each of which is different from the first identifier;	On information and belief, Prove's Contact Identification provisions contact information associated with the first identifier (e.g., phone number), wherein the contact information includes a set of different identifiers (e.g., address, name, account), each of which is different from the first identifier (e.g., phone number).

	 **The Solution** The company's call center's fraud department adopted Prove's Trust Portal solution. Trust Portal is designed to help agents, in real time, expedite manual reviews to assess risk more rapidly to better service consumers and prevent fraud. It eliminates their dependency on IT and developer teams and allows them to directly access Prove's capabilities with an intuitive, GUI-based experience. The SaaS-based, full-featured Trust Portal requires no integration, and with fast provisioning and immediate access, accelerates the organization's time to value. With Trust Portal, the company's agents can: • Verify that a caller's phone number matches their address for order delivery (Prove Identity Verification) • Measure the risk and reliability of the caller's phone number to confirm that it has not been compromised (Prove Trust Score) • Validate that the caller is in possession of the phone making the call (Prove Instant Link for Web (Fortified OTP) or Voice OTP) Using Prove's three-pronged verification and authentication approach allows the agents to expedite handle times while mitigating fraud risk. *Exhibit 18 at 2.*

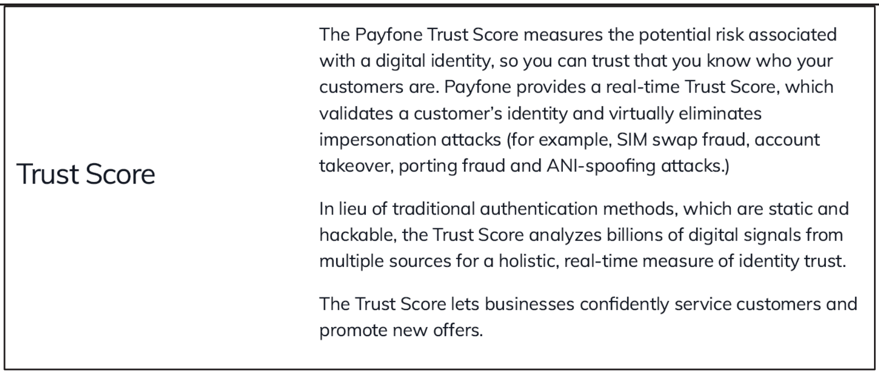
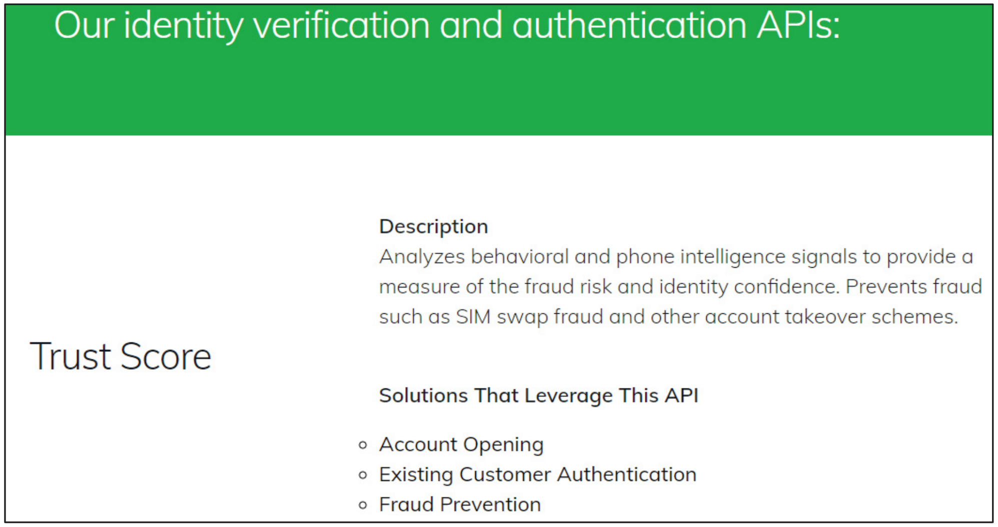
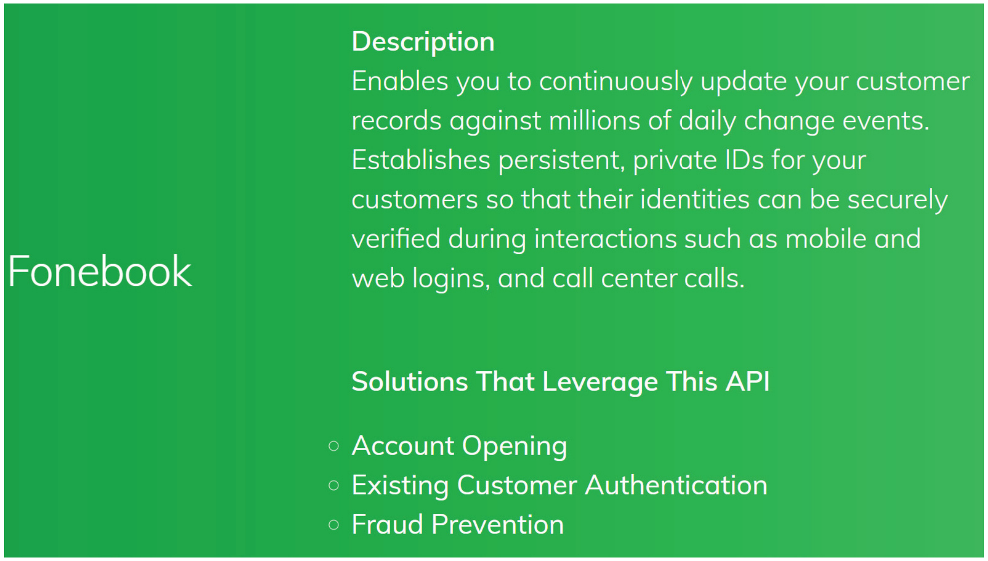
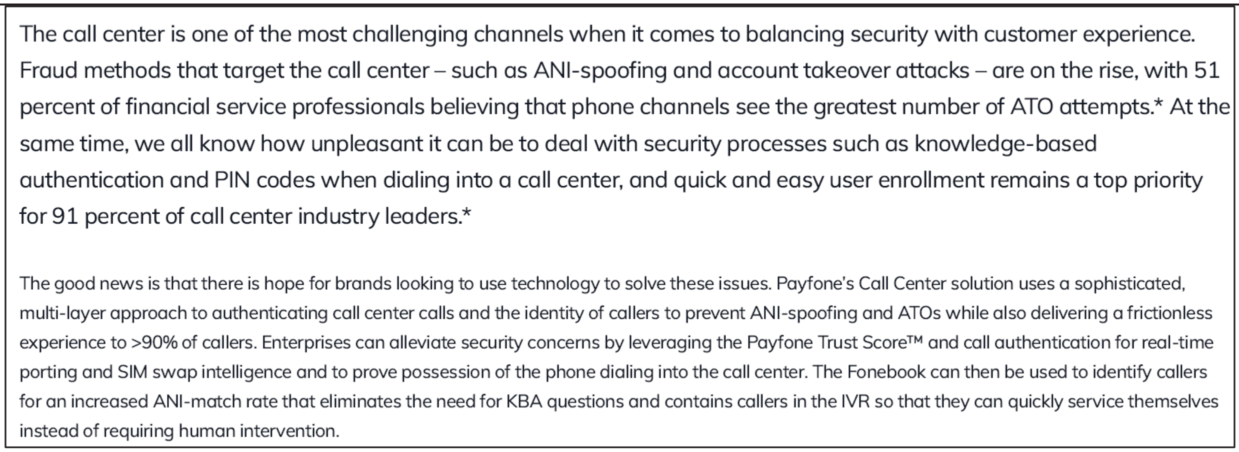
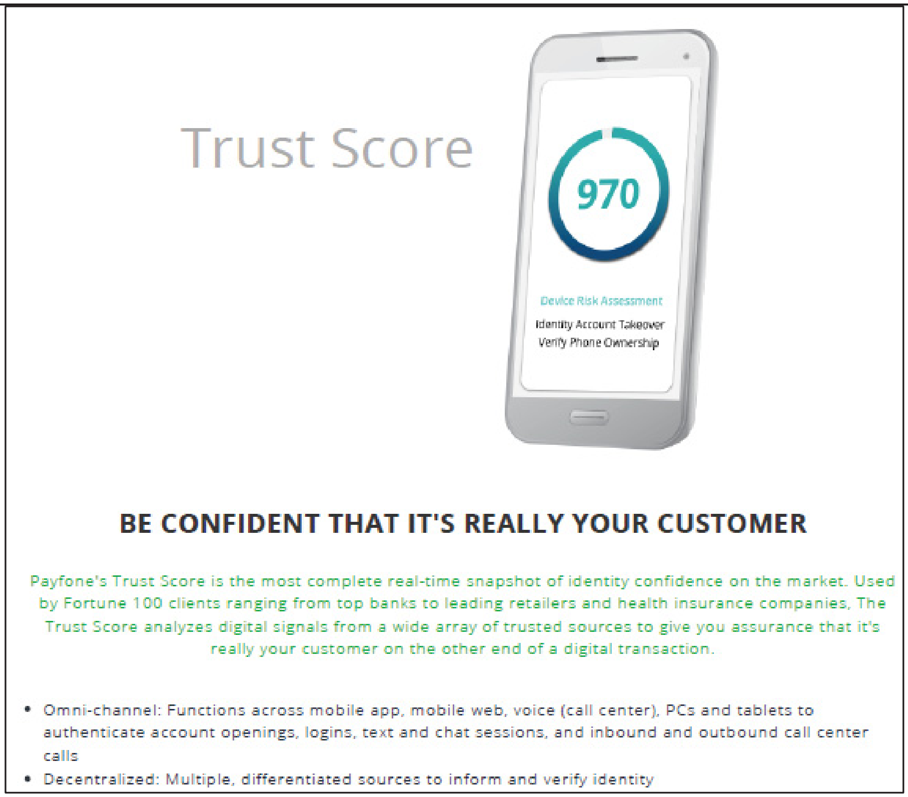
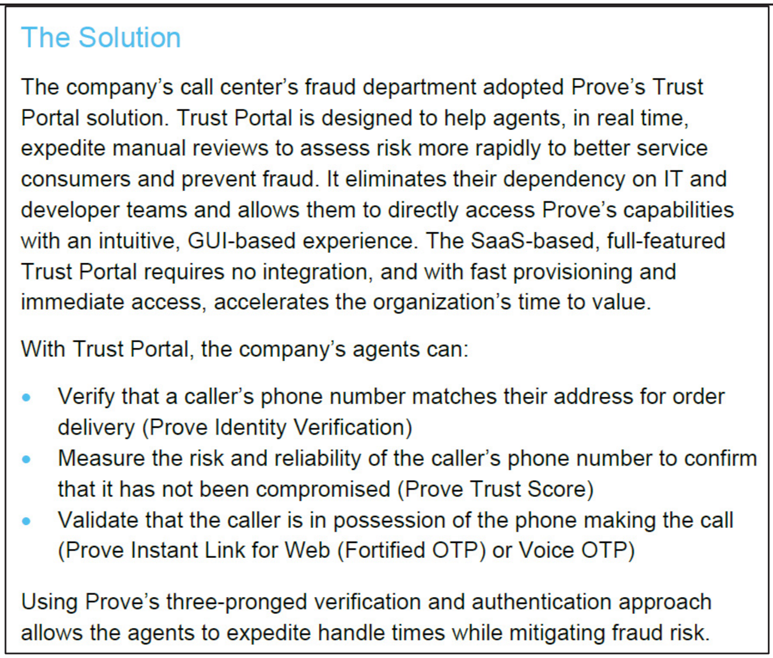
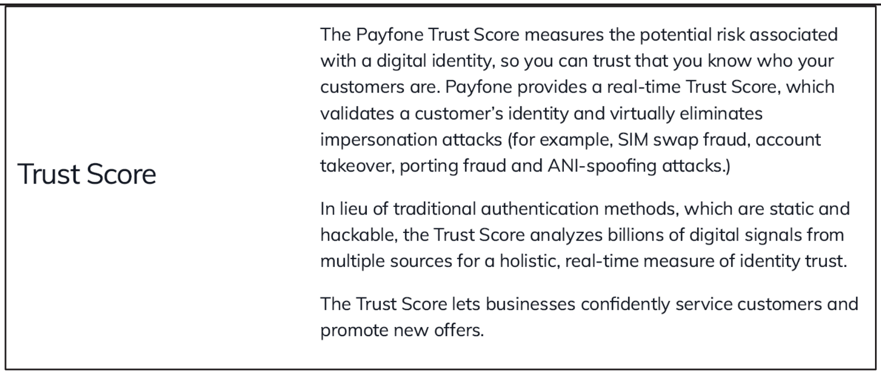
	 Trust Score The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.) In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust. The Trust Score lets businesses confidently service customers and promote new offers. *Exhibit 17 at 3.*  Our identity verification and authentication APIs: Trust Score **Description** Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes. **Solutions That Leverage This API** ○ Account Opening ○ Existing Customer Authentication ○ Fraud Prevention

	Exhibit 8 at 2. Rodger Desai indicated that Prove analyzes and stores information such as tenure of a number, behavior, and funding mechanism. *See* Consult Hyperion: Event 21 - Fireside Chat With Rodger Desai, *available at* https://chyp.com/webinars/week-21-fireside-chat-with-rodger-desai/.  Fonebook Description Enables you to continuously update your customer records against millions of daily change events. Establishes persistent, private IDs for your customers so that their identities can be securely verified during interactions such as mobile and web logins, and call center calls. Solutions That Leverage This API ○ Account Opening ○ Existing Customer Authentication ○ Fraud Prevention *Exhibit 8 at 2.*

	 The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.* The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention. *Exhibit 10 at 1.*

	 Trust Score 970 Device Risk Assessment Identity Account Takeover Verify Phone Ownership BE CONFIDENT THAT IT'S REALLY YOUR CUSTOMER Payfone's Trust Score is the most complete real-time snapshot of identity confidence on the market. Used by Fortune 100 clients ranging from top banks to leading retailers and health insurance companies, The Trust Score analyzes digital signals from a wide array of trusted sources to give you assurance that it's really your customer on the other end of a digital transaction. • Omni-channel: Functions across mobile app, mobile web, voice (call center), PCs and tablets to authenticate account openings, logins, text and chat sessions, and inbound and outbound call center calls • Decentralized: Multiple, differentiated sources to inform and verify identity *Exhibit 14 at 1.*
storing the contact information and the first identifier together in a first database;	On information and belief, Prove's Contact Identification stores the contact information and the first identifier together in a first database (e.g., Prove database).

	 The Solution The company's call center's fraud department adopted Prove's Trust Portal solution. Trust Portal is designed to help agents, in real time, expedite manual reviews to assess risk more rapidly to better service consumers and prevent fraud. It eliminates their dependency on IT and developer teams and allows them to directly access Prove's capabilities with an intuitive, GUI-based experience. The SaaS-based, full-featured Trust Portal requires no integration, and with fast provisioning and immediate access, accelerates the organization's time to value. With Trust Portal, the company's agents can: • Verify that a caller's phone number matches their address for order delivery (Prove Identity Verification) • Measure the risk and reliability of the caller's phone number to confirm that it has not been compromised (Prove Trust Score) • Validate that the caller is in possession of the phone making the call (Prove Instant Link for Web (Fortified OTP) or Voice OTP) Using Prove's three-pronged verification and authentication approach allows the agents to expedite handle times while mitigating fraud risk. *Exhibit 18 at 2.*



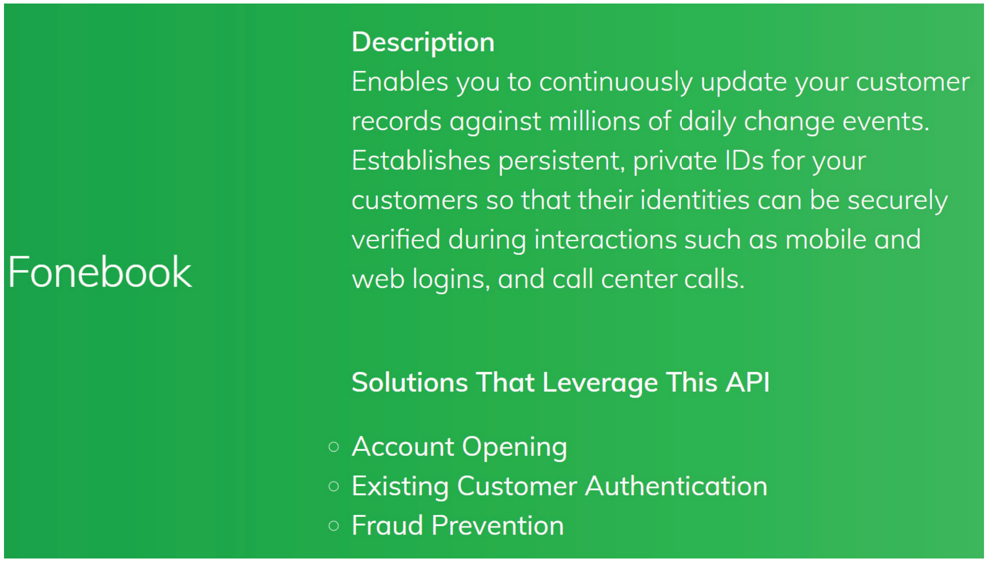
Trust Score

The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.)

In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust.

The Trust Score lets businesses confidently service customers and promote new offers.

Exhibit 17 at 3.



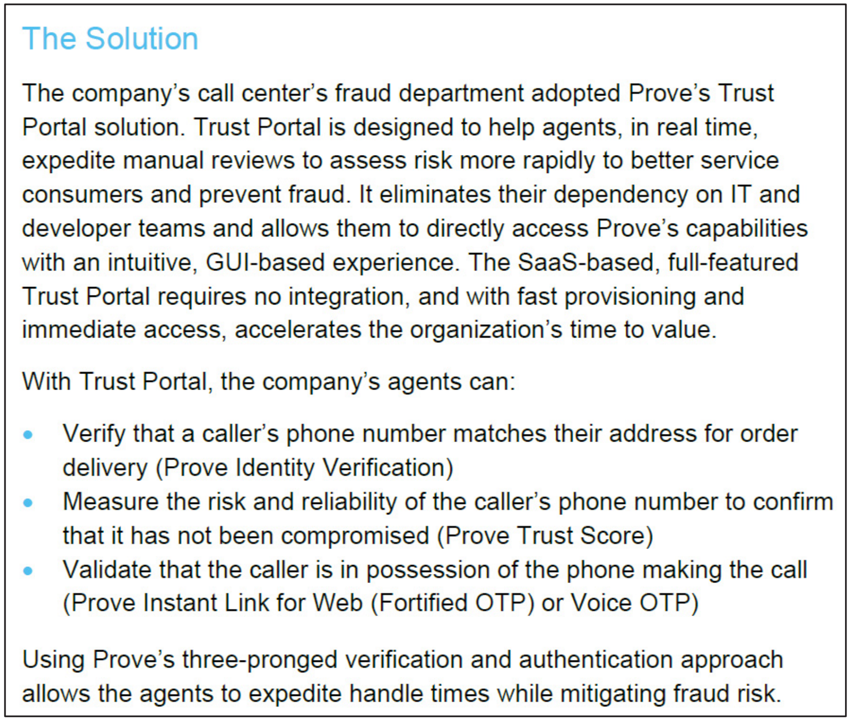
Fonebook

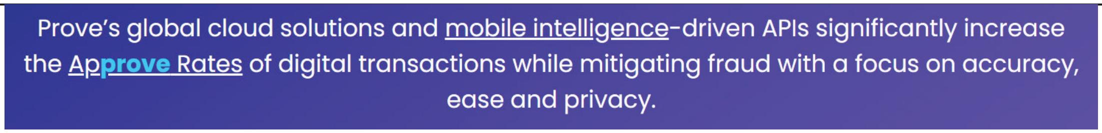
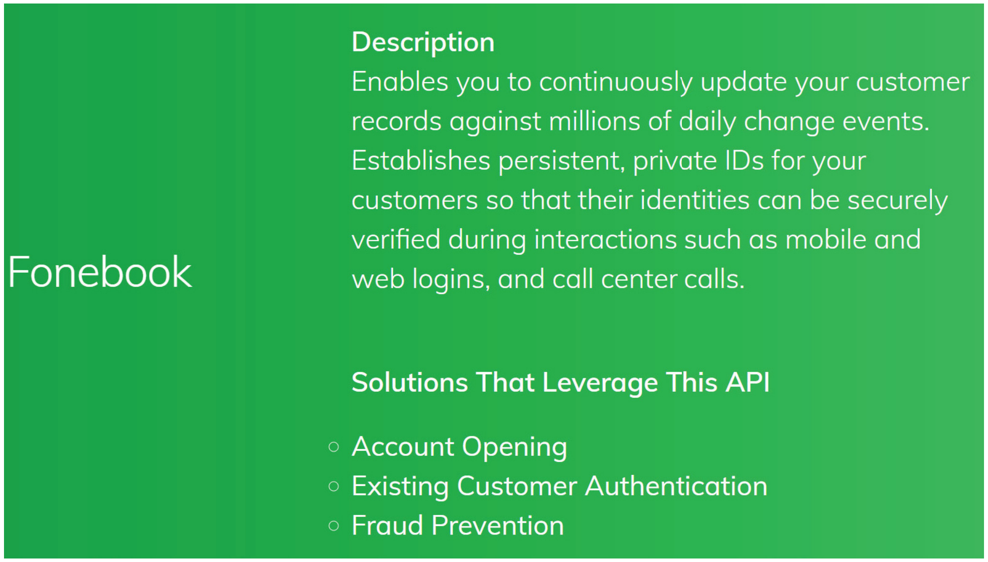
Description

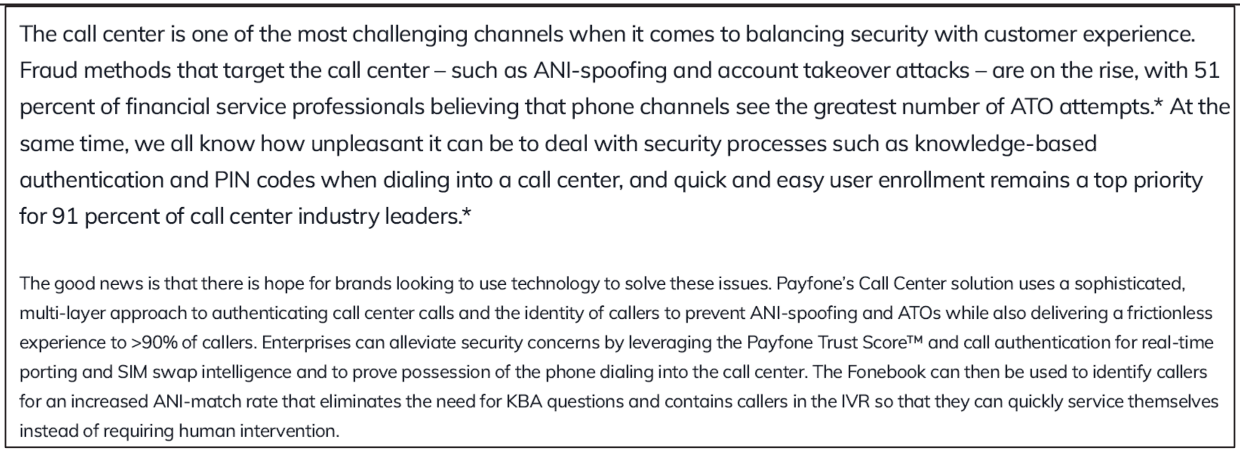
Enables you to continuously update your customer records against millions of daily change events. Establishes persistent, private IDs for your customers so that their identities can be securely verified during interactions such as mobile and web logins, and call center calls.

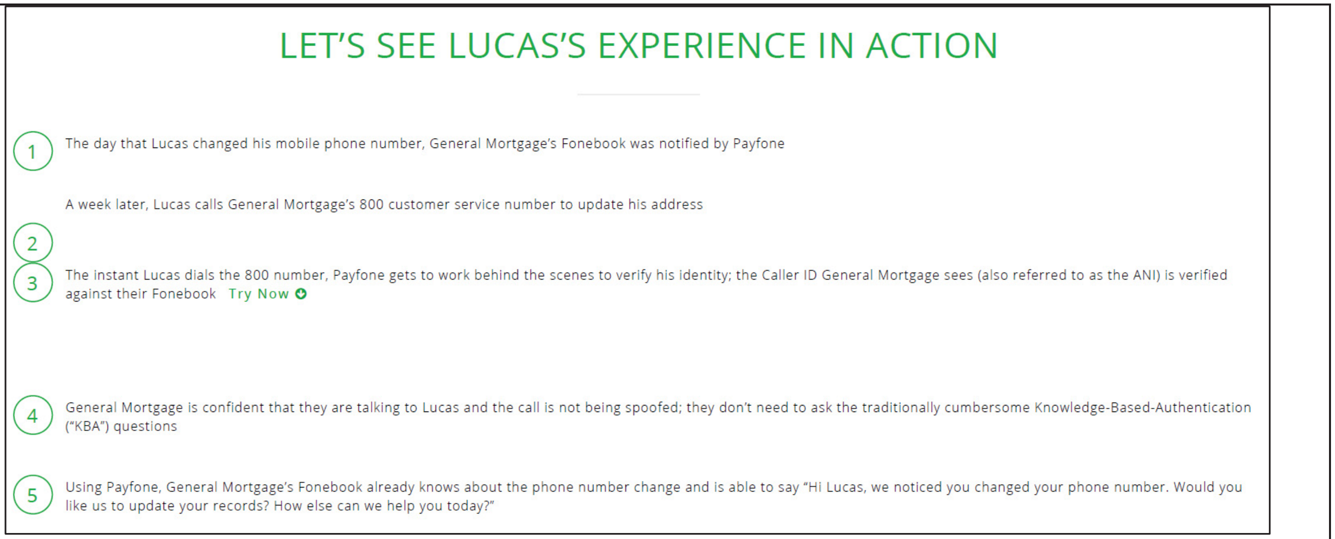
Solutions That Leverage This API

○ Account Opening
○ Existing Customer Authentication
○ Fraud Prevention

	Exhibit 8 at 2
receiving a request for the contact information from the second user, wherein a second identifier is associated with the second user;	On information and belief, Prove's Contact Identification receives a request for the contact information from the second user (e.g., call center agents, automated computer systems such as customer relationship management ("CRM") or interactive voice response ("IVR")), wherein a second identifier is associated with the second user.  The Solution The company's call center's fraud department adopted Prove's Trust Portal solution. Trust Portal is designed to help agents, in real time, expedite manual reviews to assess risk more rapidly to better service consumers and prevent fraud. It eliminates their dependency on IT and developer teams and allows them to directly access Prove's capabilities with an intuitive, GUI-based experience. The SaaS-based, full-featured Trust Portal requires no integration, and with fast provisioning and immediate access, accelerates the organization's time to value. With Trust Portal, the company's agents can: • Verify that a caller's phone number matches their address for order delivery (Prove Identity Verification) • Measure the risk and reliability of the caller's phone number to confirm that it has not been compromised (Prove Trust Score) • Validate that the caller is in possession of the phone making the call (Prove Instant Link for Web (Fortified OTP) or Voice OTP) Using Prove's three-pronged verification and authentication approach allows the agents to expedite handle times while mitigating fraud risk. *Exhibit 18 at 2.*

	 Prove's global cloud solutions and mobile intelligence-driven APIs significantly increase the Approve Rates of digital transactions while mitigating fraud with a focus on accuracy, ease and privacy. *Exhibit 19 at 1.*  Fonebook Description Enables you to continuously update your customer records against millions of daily change events. Establishes persistent, private IDs for your customers so that their identities can be securely verified during interactions such as mobile and web logins, and call center calls. Solutions That Leverage This API ○ Account Opening ○ Existing Customer Authentication ○ Fraud Prevention *Exhibit 8 at 2.*

	 The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.* The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention. *Exhibit 10 at 1.*



LET'S SEE LUCAS'S EXPERIENCE IN ACTION

1. The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone

   A week later, Lucas calls General Mortgage's 800 customer service number to update his address

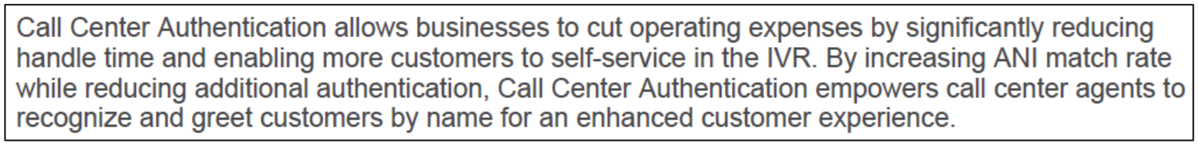
2.

3. The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now ➲

4. General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions

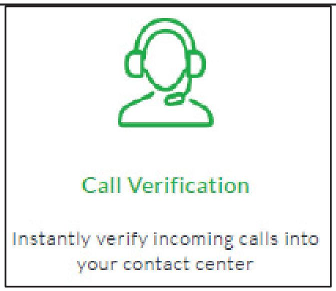
5. Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?"

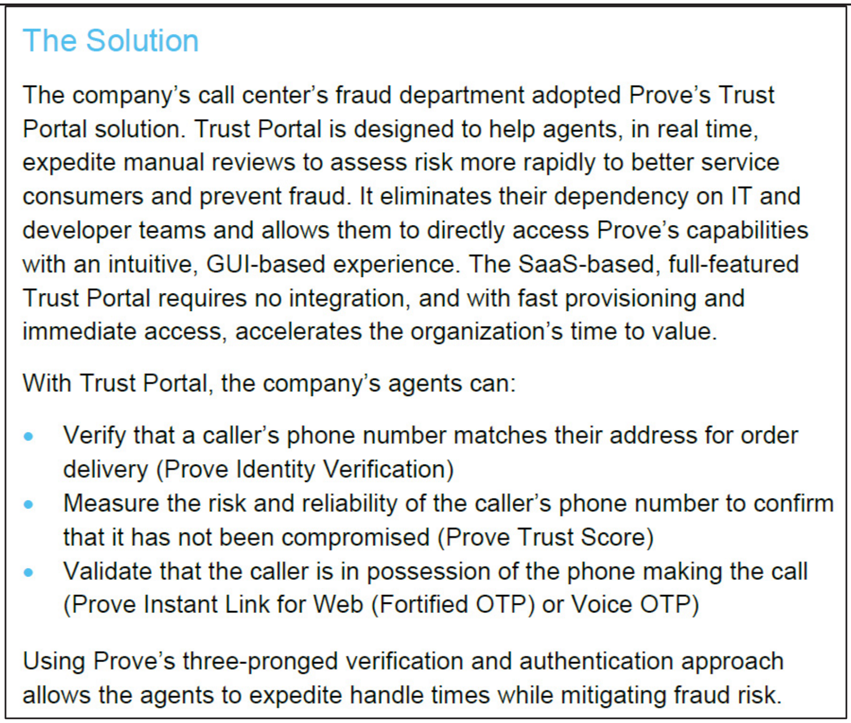
Exhibit 13 at 1.



Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience.

Exhibit 9 at 2.

	 Call Verification Instantly verify incoming calls into your contact center *Exhibit 21 at 1.*
determining whether the second user is authorized to obtain the contact information, based on the second identifier being in a set of authorized identifiers authorized to access the contact information;	On information and belief, Prove's Contact Identification determines whether the second user (e.g., call center agents, automated computer systems such as customer relationship management ("CRM") or interactive voice response ("IVR")) is authorized to obtain the contact information, based on the second identifier being in a set of authorized identifiers authorized to access the contact information.



The Solution

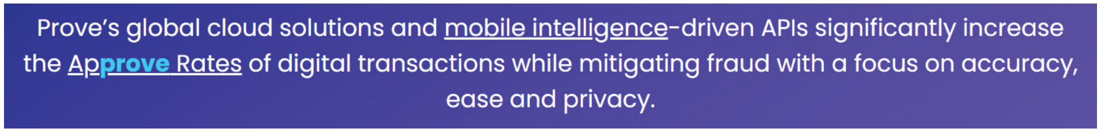
The company's call center's fraud department adopted Prove's Trust Portal solution. Trust Portal is designed to help agents, in real time, expedite manual reviews to assess risk more rapidly to better service consumers and prevent fraud. It eliminates their dependency on IT and developer teams and allows them to directly access Prove's capabilities with an intuitive, GUI-based experience. The SaaS-based, full-featured Trust Portal requires no integration, and with fast provisioning and immediate access, accelerates the organization's time to value.

With Trust Portal, the company's agents can:

- Verify that a caller's phone number matches their address for order delivery (Prove Identity Verification)
- Measure the risk and reliability of the caller's phone number to confirm that it has not been compromised (Prove Trust Score)
- Validate that the caller is in possession of the phone making the call (Prove Instant Link for Web (Fortified OTP) or Voice OTP)

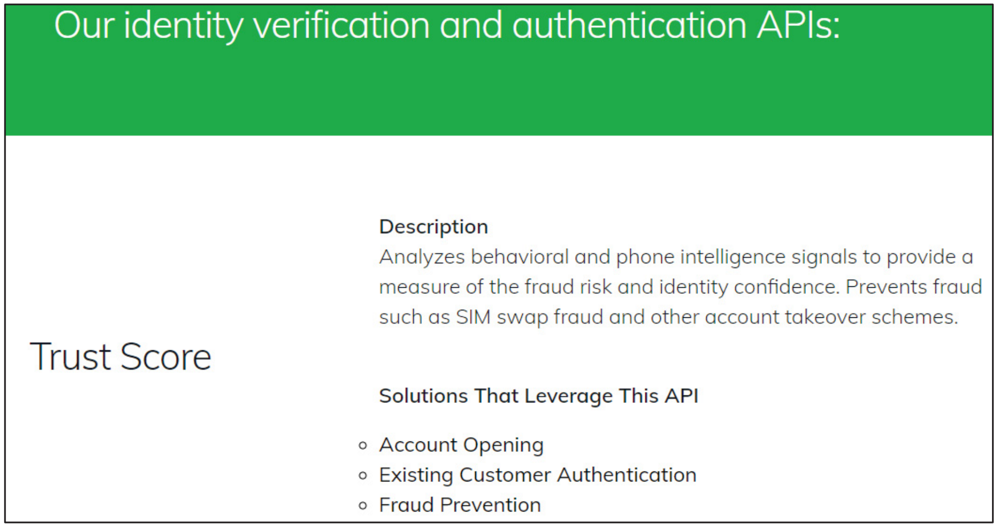
Using Prove's three-pronged verification and authentication approach allows the agents to expedite handle times while mitigating fraud risk.

Exhibit 18 at 2.



Prove's global cloud solutions and mobile intelligence-driven APIs significantly increase the Approve Rates of digital transactions while mitigating fraud with a focus on accuracy, ease and privacy.

Exhibit 19 at 1.



Our identity verification and authentication APIs:

Trust Score

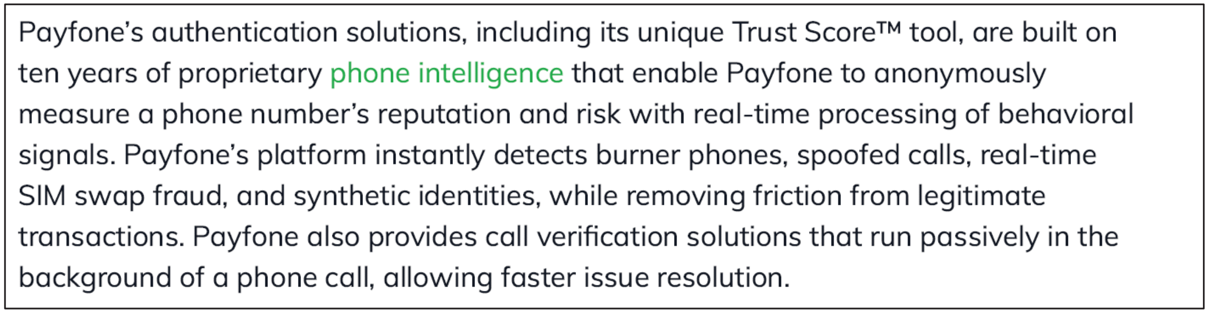
Description

Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes.

Solutions That Leverage This API

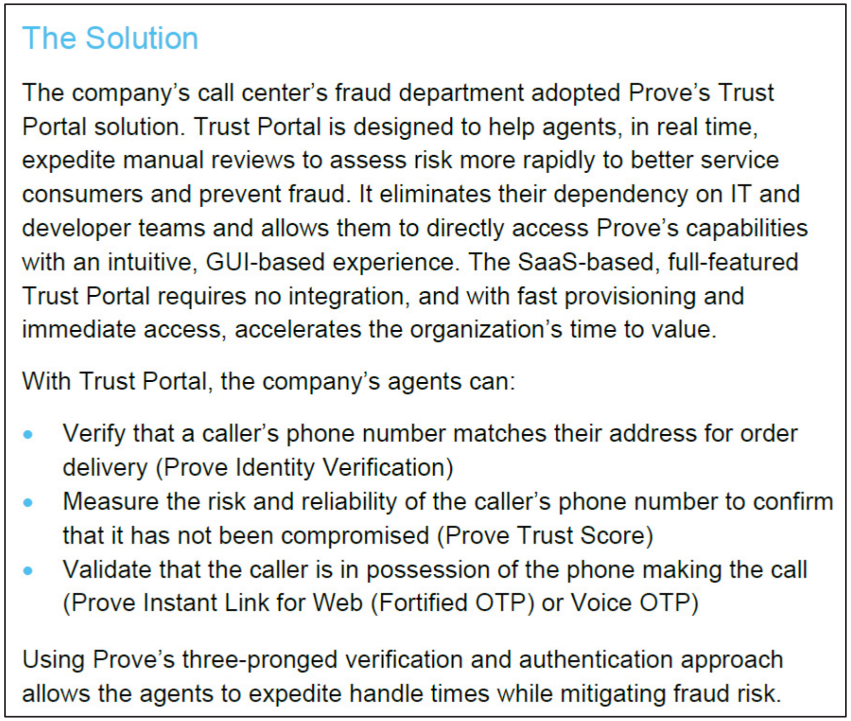
- Account Opening
- Existing Customer Authentication
- Fraud Prevention

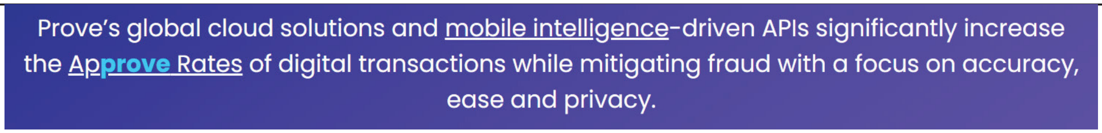
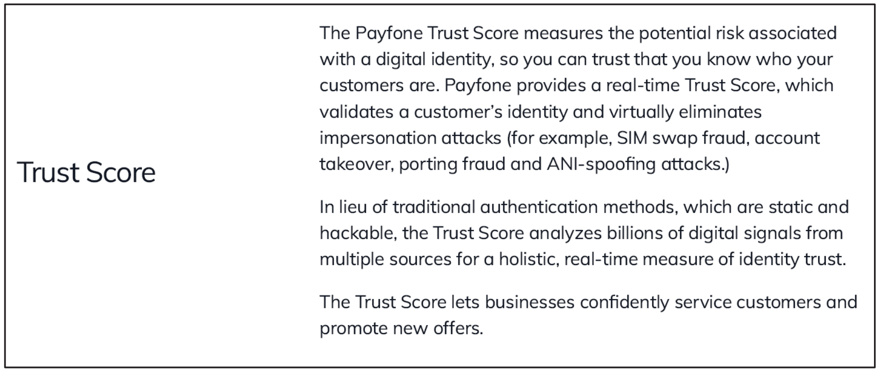
Exhibit 8 at 2.

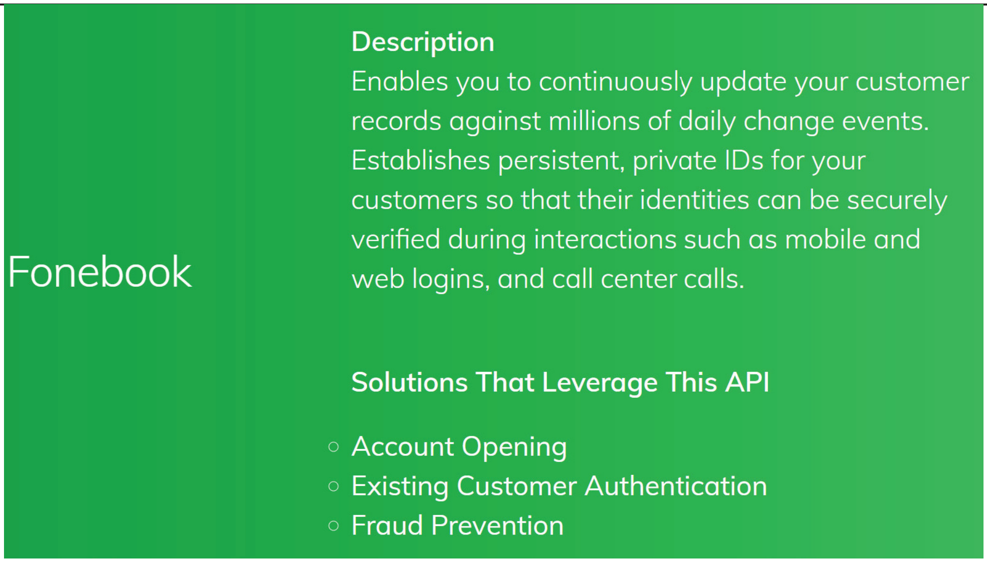
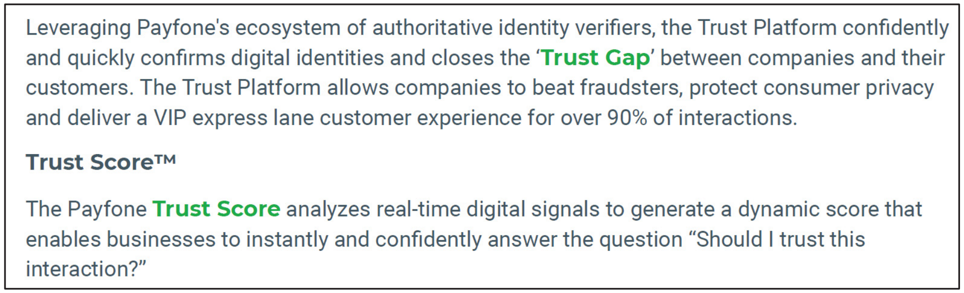


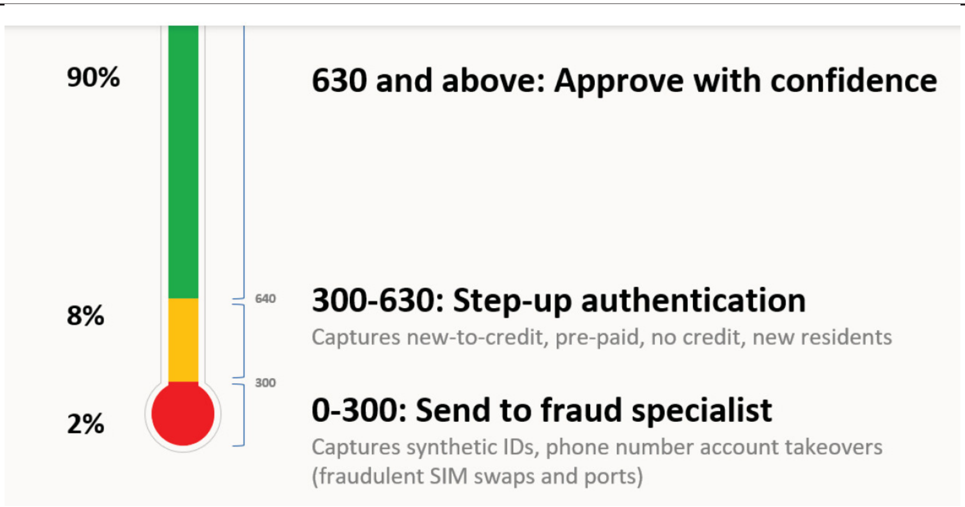
Payfone's authentication solutions, including its unique Trust Score™ tool, are built on ten years of proprietary phone intelligence that enable Payfone to anonymously measure a phone number's reputation and risk with real-time processing of behavioral signals. Payfone's platform instantly detects burner phones, spoofed calls, real-time SIM swap fraud, and synthetic identities, while removing friction from legitimate transactions. Payfone also provides call verification solutions that run passively in the background of a phone call, allowing faster issue resolution.

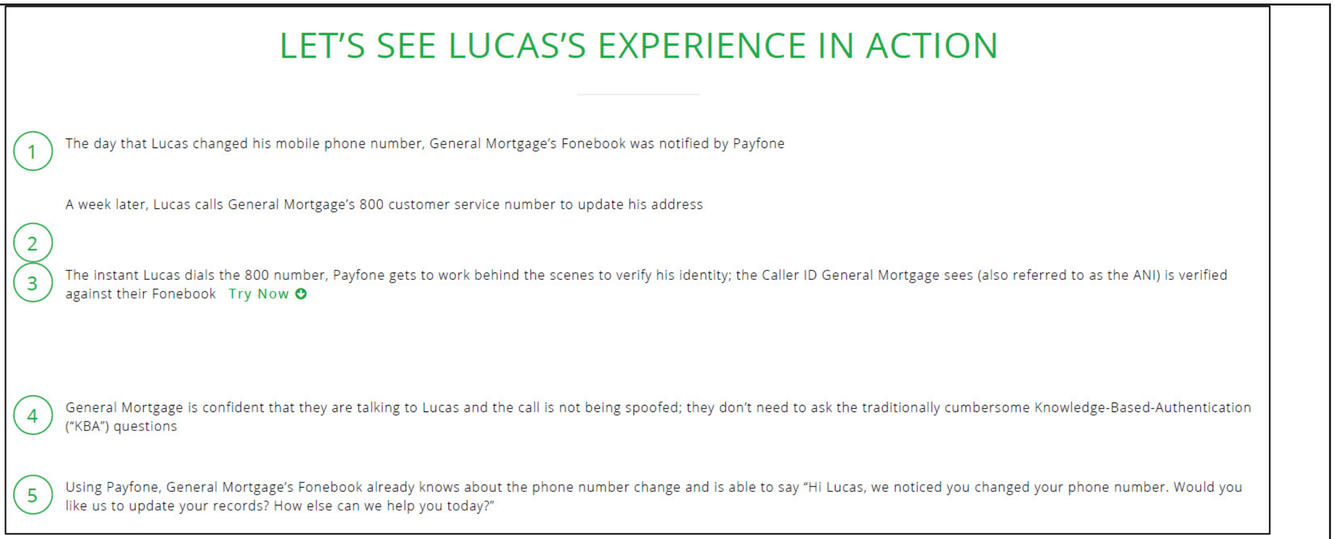
Exhibit 15 at 2.

when a determination is made that the second user is authorized to obtain the contact information, retrieving the contact information from the first database; and	On information and belief, Prove's Contact Identification includes, when a determination is made that the second user (e.g., call center agents, automated computer systems such as customer relationship management ("CRM") or interactive voice response ("IVR")) is authorized to obtain the contact information, retrieving the contact information from the first database.  The Solution The company's call center's fraud department adopted Prove's Trust Portal solution. Trust Portal is designed to help agents, in real time, expedite manual reviews to assess risk more rapidly to better service consumers and prevent fraud. It eliminates their dependency on IT and developer teams and allows them to directly access Prove's capabilities with an intuitive, GUI-based experience. The SaaS-based, full-featured Trust Portal requires no integration, and with fast provisioning and immediate access, accelerates the organization's time to value. With Trust Portal, the company's agents can: • Verify that a caller's phone number matches their address for order delivery (Prove Identity Verification) • Measure the risk and reliability of the caller's phone number to confirm that it has not been compromised (Prove Trust Score) • Validate that the caller is in possession of the phone making the call (Prove Instant Link for Web (Fortified OTP) or Voice OTP) Using Prove's three-pronged verification and authentication approach allows the agents to expedite handle times while mitigating fraud risk. *Exhibit 18 at 2.*

	 Prove's global cloud solutions and mobile intelligence-driven APIs significantly increase the Approve Rates of digital transactions while mitigating fraud with a focus on accuracy, ease and privacy. *Exhibit 19 at 1.*  Trust Score The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.) In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust. The Trust Score lets businesses confidently service customers and promote new offers. *Exhibit 17 at 3.*

	 Fonebook **Description** Enables you to continuously update your customer records against millions of daily change events. Establishes persistent, private IDs for your customers so that their identities can be securely verified during interactions such as mobile and web logins, and call center calls. **Solutions That Leverage This API** ○ Account Opening ○ Existing Customer Authentication ○ Fraud Prevention *Exhibit 8 at 2.*  Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the '**Trust Gap**' between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions. **Trust Score™** The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question "Should I trust this interaction?" *Exhibit 11 at 4.*

	 **630 and above: Approve with confidence** **300-630: Step-up authentication** Captures new-to-credit, pre-paid, no credit, new residents **0-300: Send to fraud specialist** Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports) *Exhibit 11 at 5.*



LET'S SEE LUCAS'S EXPERIENCE IN ACTION

1 The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone

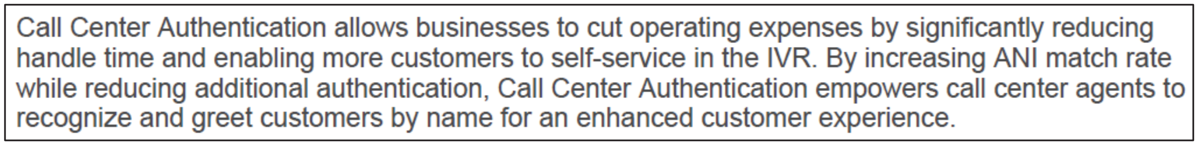
2 A week later, Lucas calls General Mortgage's 800 customer service number to update his address

3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook

4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions

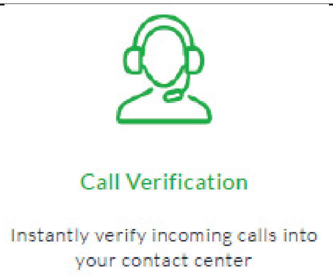
5 Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?"

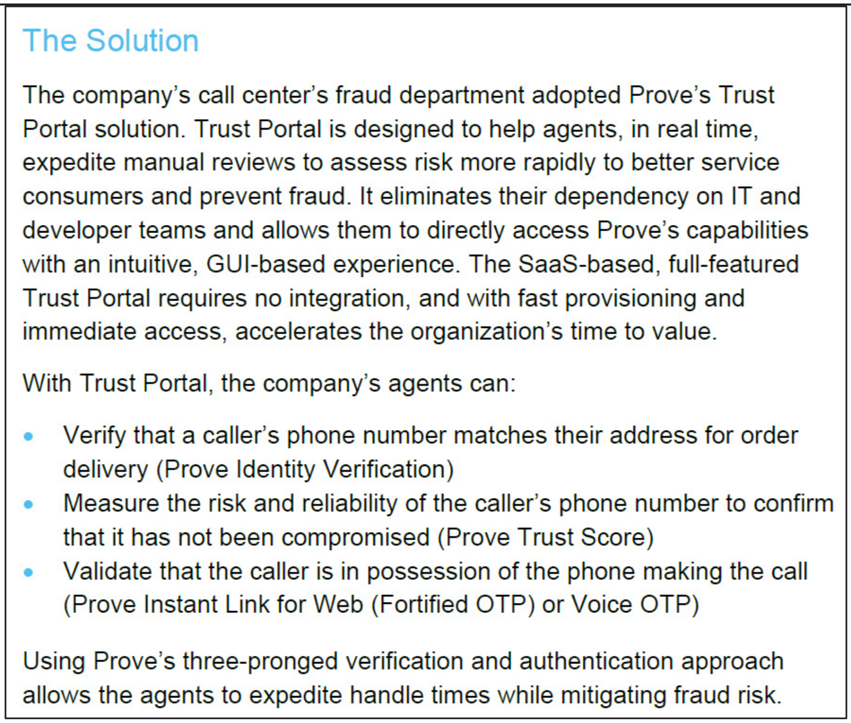
Exhibit 13 at 1.

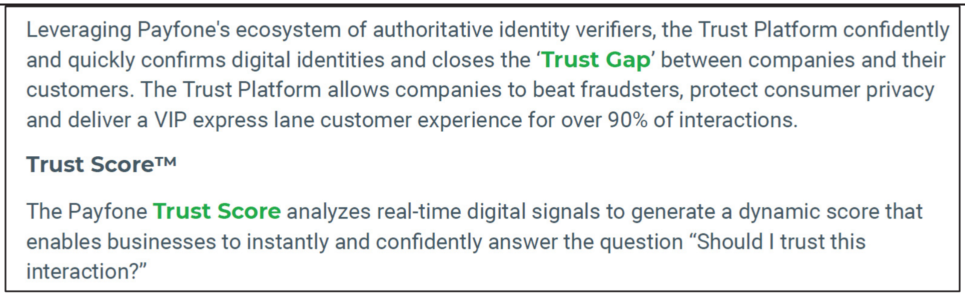


Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience.

Exhibit 9 at 2.

	 Call Verification Instantly verify incoming calls into your contact center *Exhibit 21 at 1.*
transmitting the contact information to the second application associated with the second user without receiving an authorization signal from the first user in response to the request.	On information and belief, Prove's Contact Identification transmitting the contact information to the second application associated with the second user without receiving an authorization signal from the first user (e.g., caller) in response to the request.

	The Solution The company's call center's fraud department adopted Prove's Trust Portal solution. Trust Portal is designed to help agents, in real time, expedite manual reviews to assess risk more rapidly to better service consumers and prevent fraud. It eliminates their dependency on IT and developer teams and allows them to directly access Prove's capabilities with an intuitive, GUI-based experience. The SaaS-based, full-featured Trust Portal requires no integration, and with fast provisioning and immediate access, accelerates the organization's time to value. With Trust Portal, the company's agents can: • Verify that a caller's phone number matches their address for order delivery (Prove Identity Verification) • Measure the risk and reliability of the caller's phone number to confirm that it has not been compromised (Prove Trust Score) • Validate that the caller is in possession of the phone making the call (Prove Instant Link for Web (Fortified OTP) or Voice OTP) Using Prove's three-pronged verification and authentication approach allows the agents to expedite handle times while mitigating fraud risk. *Exhibit 18 at 2.*

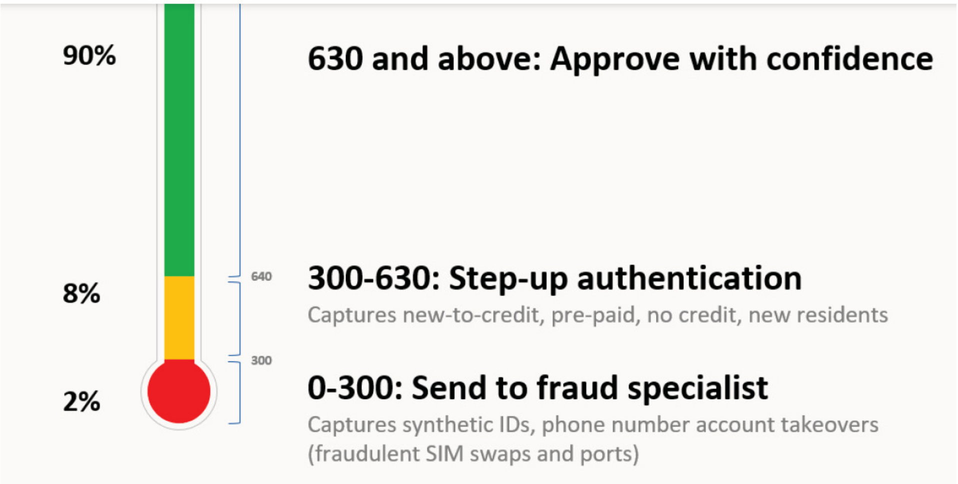


Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the '**Trust Gap**' between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions.

Trust Score™

The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question "Should I trust this interaction?"

Exhibit 11 at 4.



630 and above: Approve with confidence

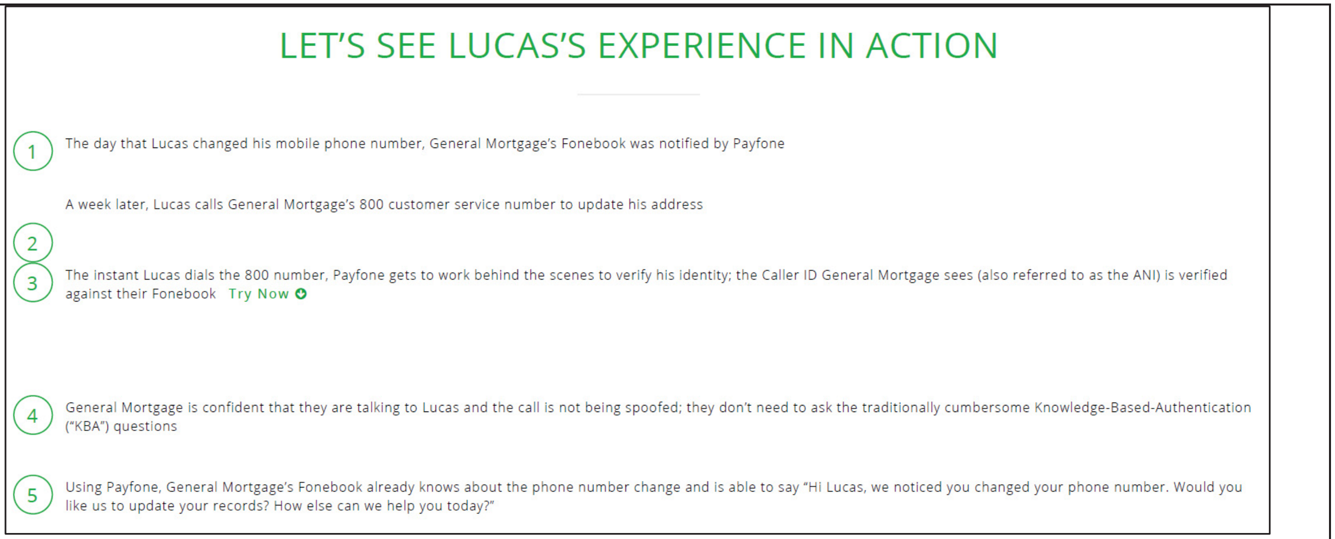
300-630: Step-up authentication

Captures new-to-credit, pre-paid, no credit, new residents

0-300: Send to fraud specialist

Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports)

Exhibit 11 at 5.



LET'S SEE LUCAS'S EXPERIENCE IN ACTION

1 The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone

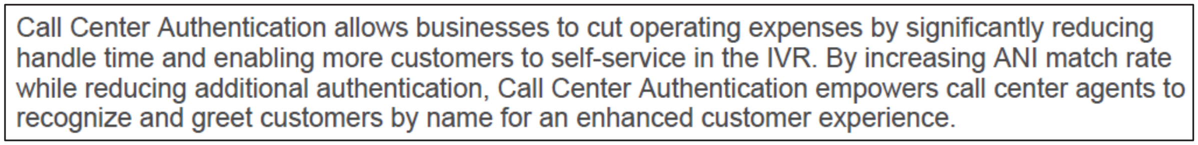
2 A week later, Lucas calls General Mortgage's 800 customer service number to update his address

3 The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now

4 General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions

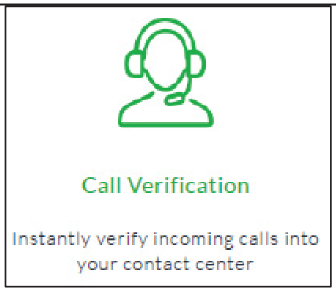
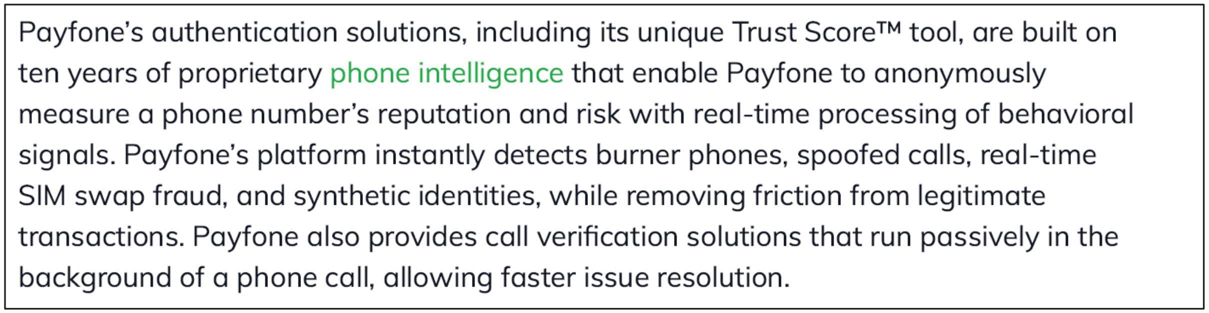
5 Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?"

Exhibit 13 at 1.



Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience.

Exhibit 9 at 2.

	 Call Verification Instantly verify incoming calls into your contact center *Exhibit 21 at 1.*  Payfone's authentication solutions, including its unique Trust Score™ tool, are built on ten years of proprietary phone intelligence that enable Payfone to anonymously measure a phone number's reputation and risk with real-time processing of behavioral signals. Payfone's platform instantly detects burner phones, spoofed calls, real-time SIM swap fraud, and synthetic identities, while removing friction from legitimate transactions. Payfone also provides call verification solutions that run passively in the background of a phone call, allowing faster issue resolution. *Exhibit 15 at 2.*

**PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT**

<table>
<tr>
<td></td>
<td>

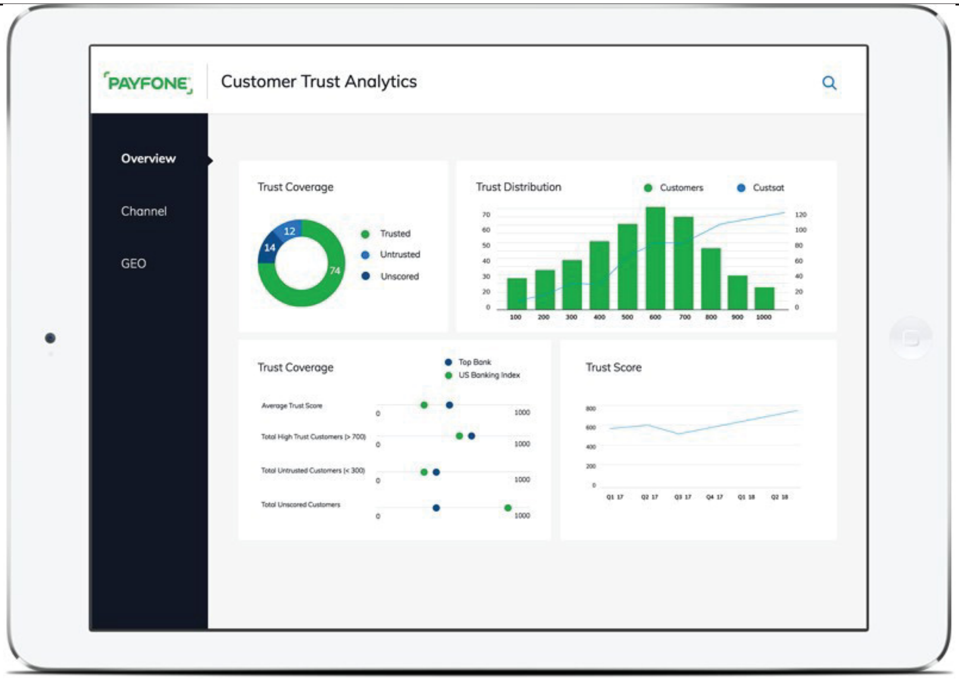
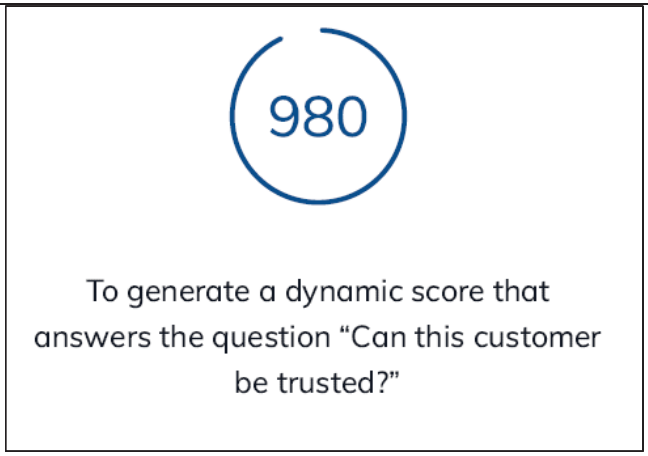


Exhibit 20 at 1.

</td>
</tr>
</table>

	 To generate a dynamic score that answers the question "Can this customer be trusted?" *Exhibit 17 at 3.*

PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT

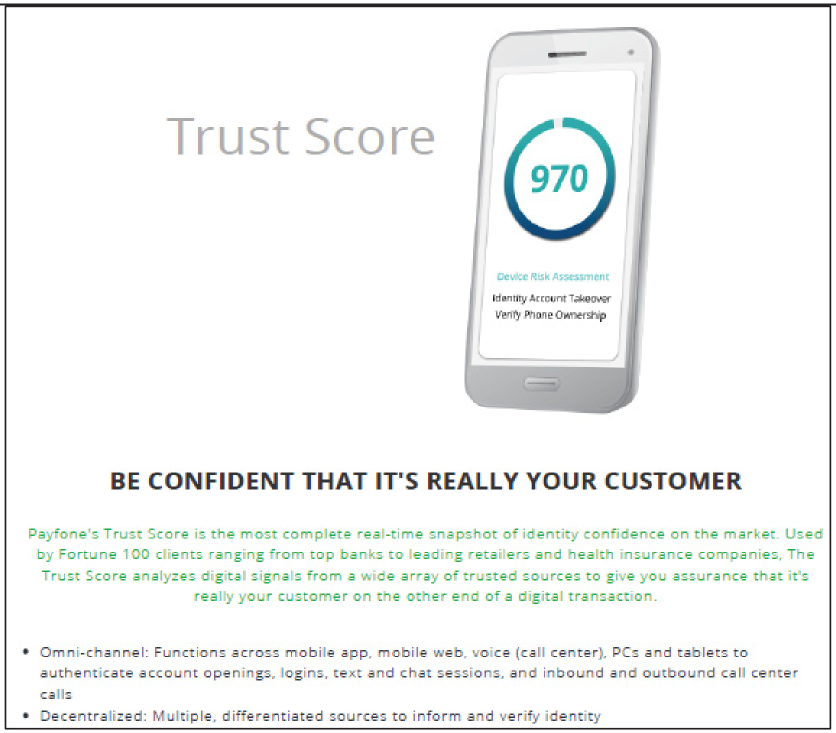
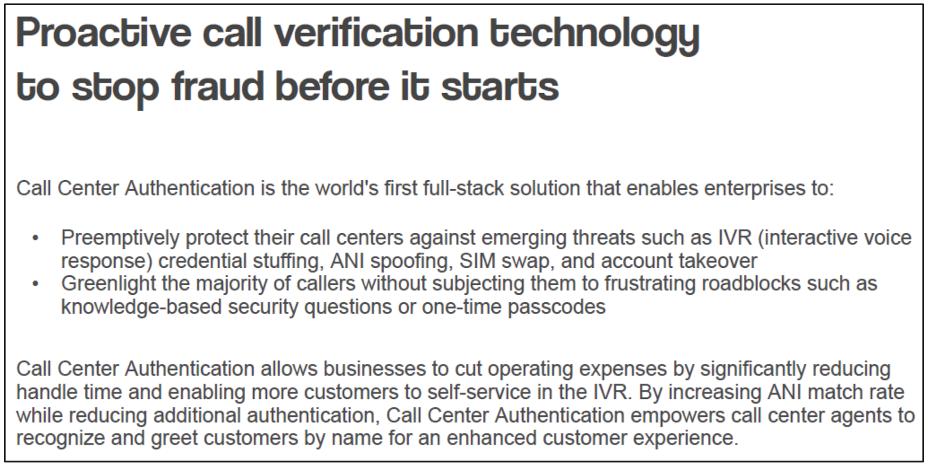
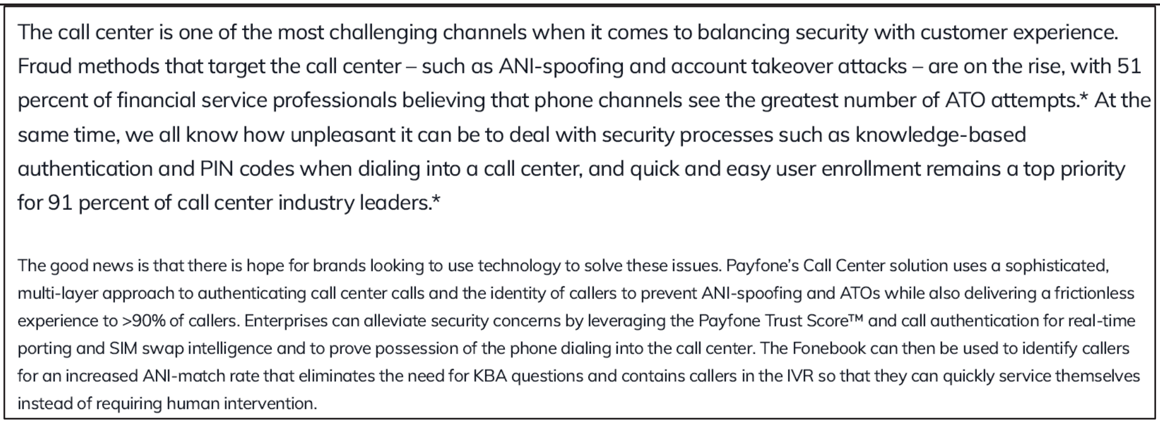
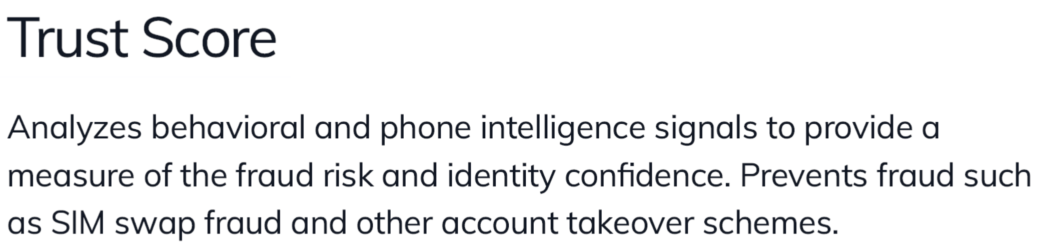
	 970 Device Risk Assessment Identity Account Takeover Verify Phone Ownership Trust Score **BE CONFIDENT THAT IT'S REALLY YOUR CUSTOMER** Payfone's Trust Score is the most complete real-time snapshot of identity confidence on the market. Used by Fortune 100 clients ranging from top banks to leading retailers and health insurance companies. The Trust Score analyzes digital signals from a wide array of trusted sources to give you assurance that it's really your customer on the other end of a digital transaction. • Omni-channel: Functions across mobile app, mobile web, voice (call center), PCs and tablets to authenticate account openings, logins, text and chat sessions, and inbound and outbound call center calls • Decentralized: Multiple, differentiated sources to inform and verify identity *Exhibit 14 at 1.*

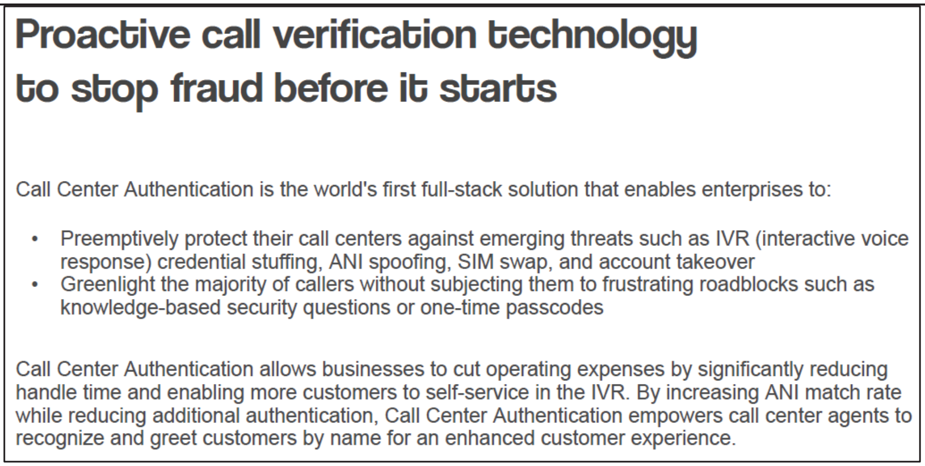
Exhibit 27

US 10,547,739 Claim 1

Prove's Call Center Authentication and Contact Identification

1. A method for operating a computing device, the method comprising:	Prove's Call Center Authentication includes a method for operating a computing device.  **Proactive call verification technology to stop fraud before it starts** Call Center Authentication is the world's first full-stack solution that enables enterprises to: • Preemptively protect their call centers against emerging threats such as IVR (interactive voice response) credential stuffing, ANI spoofing, SIM swap, and account takeover • Greenlight the majority of callers without subjecting them to frustrating roadblocks such as knowledge-based security questions or one-time passcodes Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience. *Exhibit 9 at 2.*

	 The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.* The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention. *Exhibit 10 at 1.*  Trust Score Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes. *Exhibit 8 at 1-2.*
(a) determining a phone number of an incoming communication;	Prove's Call Center Authentication determines a phone number of an incoming communication (e.g., ANI).



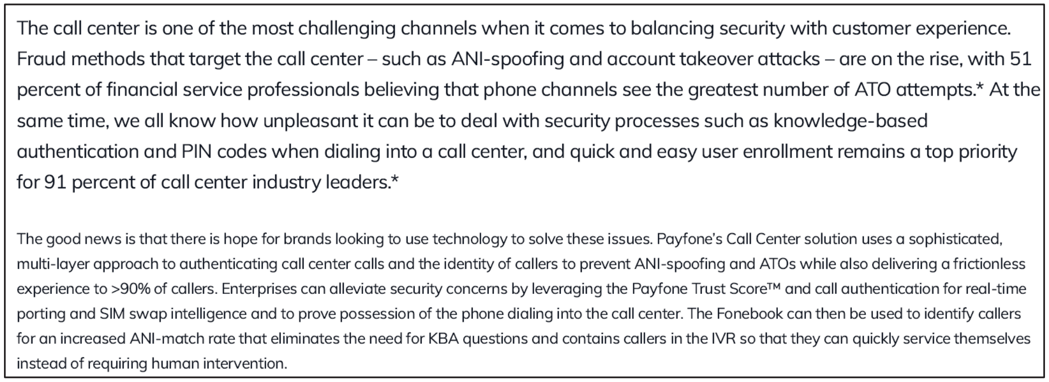
Proactive call verification technology to stop fraud before it starts

Call Center Authentication is the world's first full-stack solution that enables enterprises to:

- Preemptively protect their call centers against emerging threats such as IVR (interactive voice response) credential stuffing, ANI spoofing, SIM swap, and account takeover
- Greenlight the majority of callers without subjecting them to frustrating roadblocks such as knowledge-based security questions or one-time passcodes

Call Center Authentication allows businesses to cut operating expenses by significantly reducing handle time and enabling more customers to self-service in the IVR. By increasing ANI match rate while reducing additional authentication, Call Center Authentication empowers call center agents to recognize and greet customers by name for an enhanced customer experience.

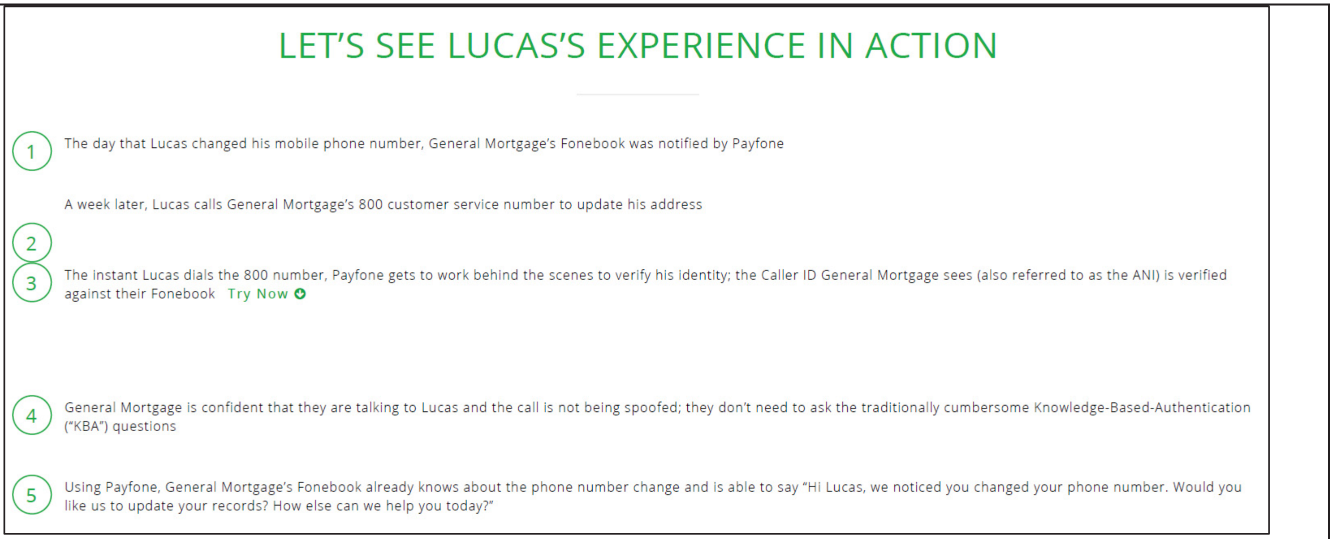
Exhibit 9 at 2.



The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.*

The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention.

Exhibit 10 at 1.



LET'S SEE LUCAS'S EXPERIENCE IN ACTION

1. The day that Lucas changed his mobile phone number, General Mortgage's Fonebook was notified by Payfone

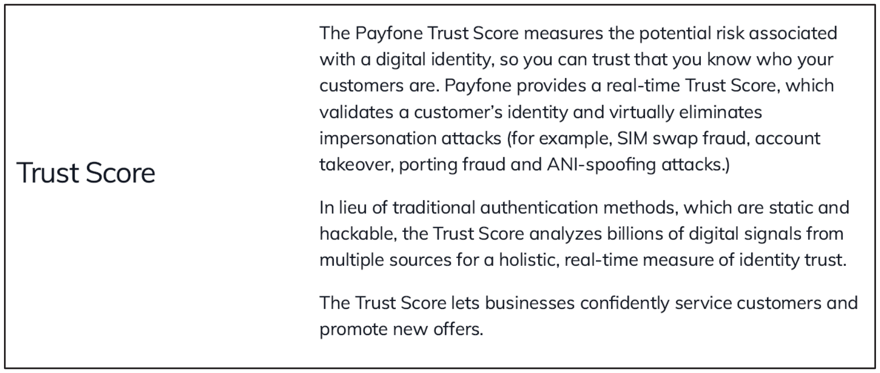
A week later, Lucas calls General Mortgage's 800 customer service number to update his address

2.
3. The instant Lucas dials the 800 number, Payfone gets to work behind the scenes to verify his identity; the Caller ID General Mortgage sees (also referred to as the ANI) is verified against their Fonebook Try Now ⊕

4. General Mortgage is confident that they are talking to Lucas and the call is not being spoofed; they don't need to ask the traditionally cumbersome Knowledge-Based-Authentication ("KBA") questions

5. Using Payfone, General Mortgage's Fonebook already knows about the phone number change and is able to say "Hi Lucas, we noticed you changed your phone number. Would you like us to update your records? How else can we help you today?"

Exhibit 13 at 1.



Trust Score

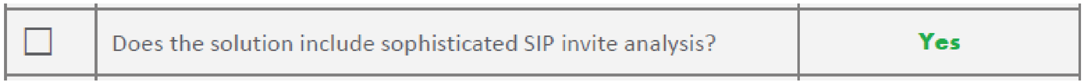
The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.)

In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust.

The Trust Score lets businesses confidently service customers and promote new offers.

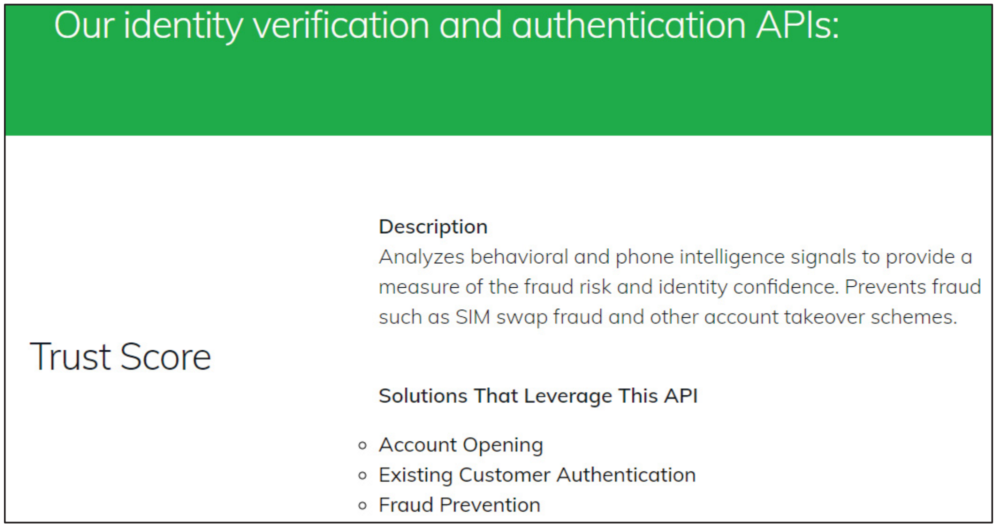
**PRIVILEGED AND CONFIDENTIAL /
ATTORNEY CLIENT WORK PRODUCT**

Exhibit 17 at 3.



□	Does the solution include sophisticated SIP invite analysis?	Yes

Exhibit 12 at 1.



Our identity verification and authentication APIs:

Trust Score

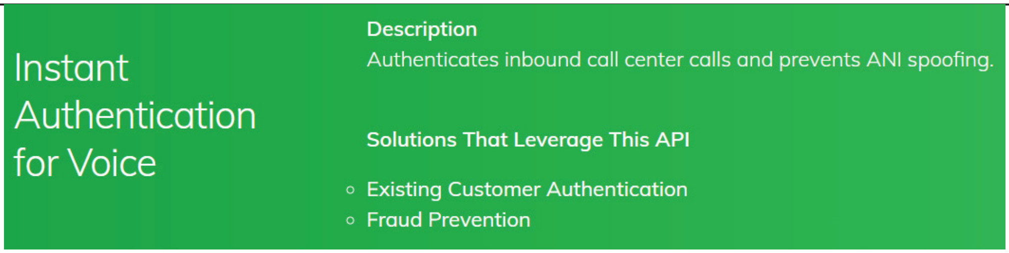
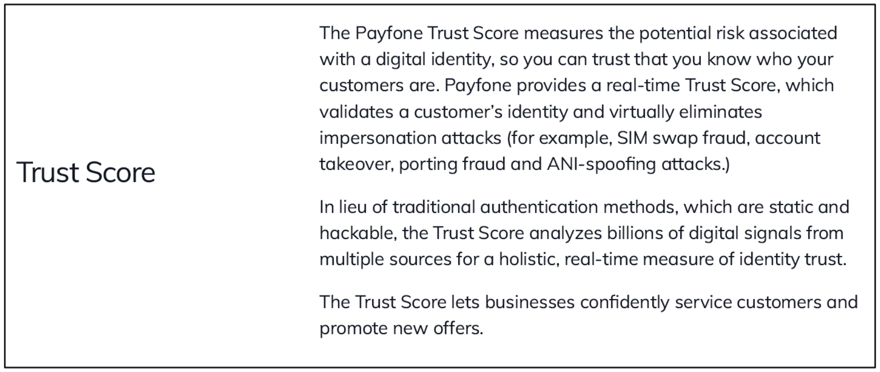
Description

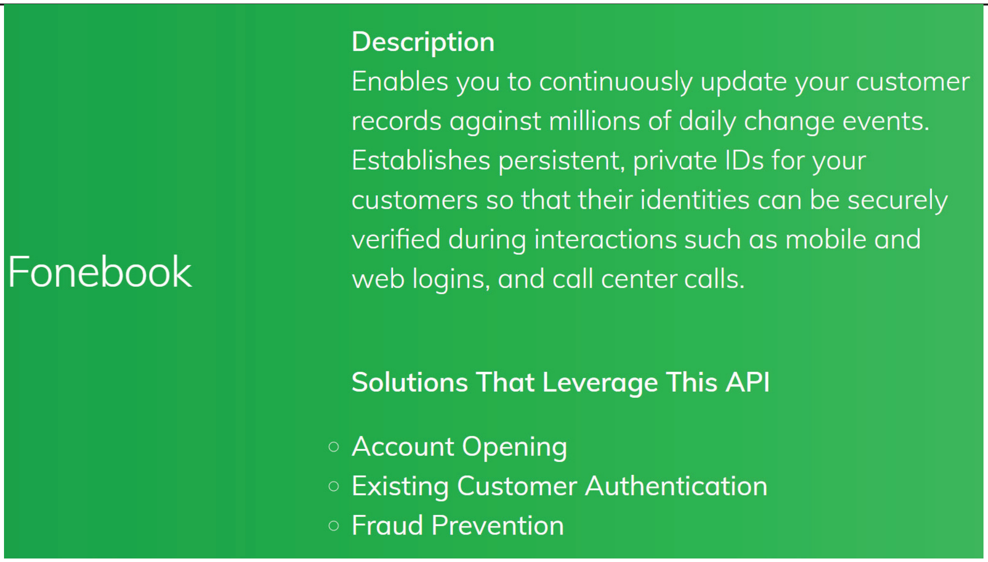
Analyzes behavioral and phone intelligence signals to provide a measure of the fraud risk and identity confidence. Prevents fraud such as SIM swap fraud and other account takeover schemes.

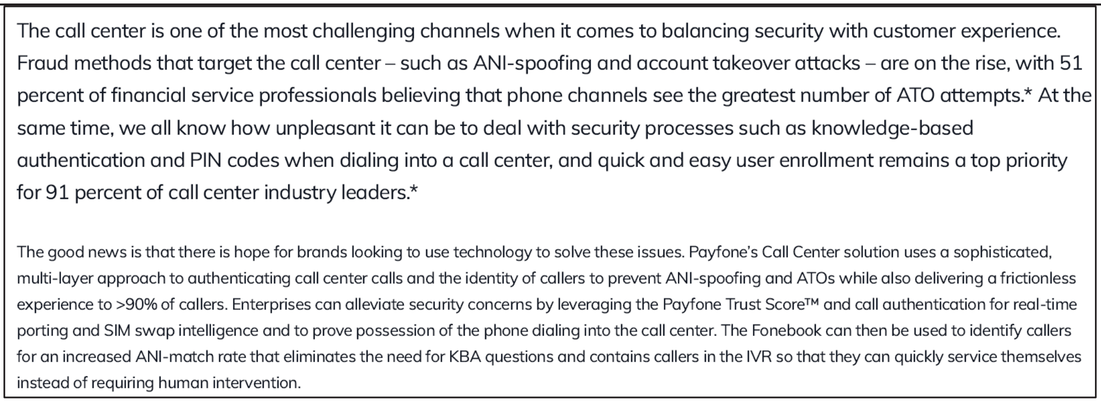
Solutions That Leverage This API

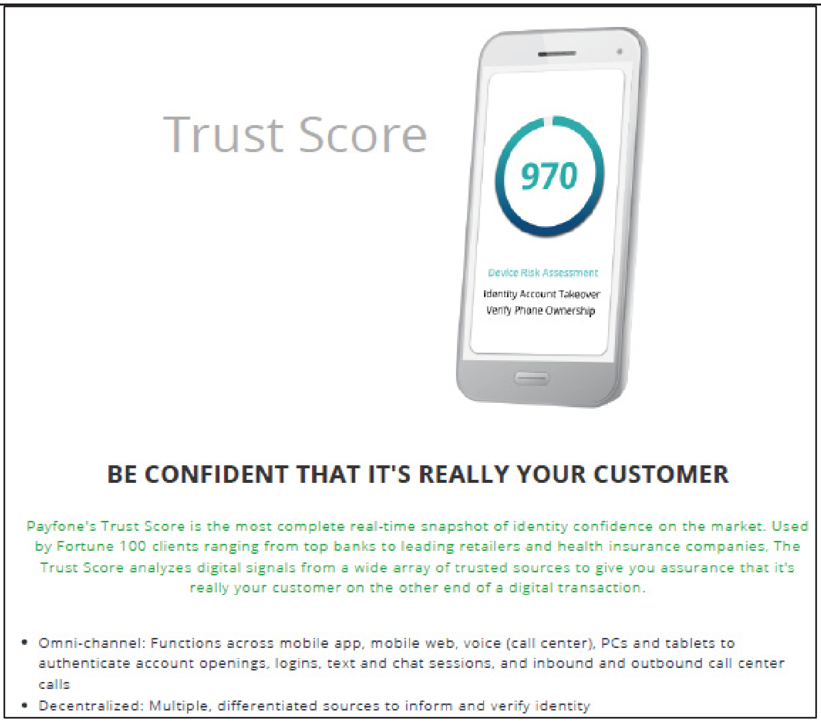
- Account Opening
- Existing Customer Authentication
- Fraud Prevention

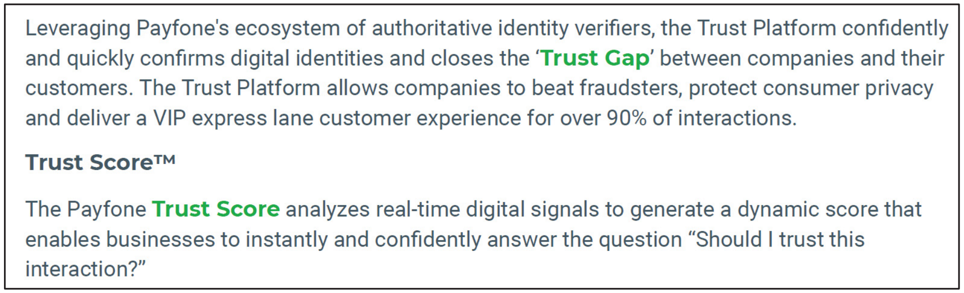
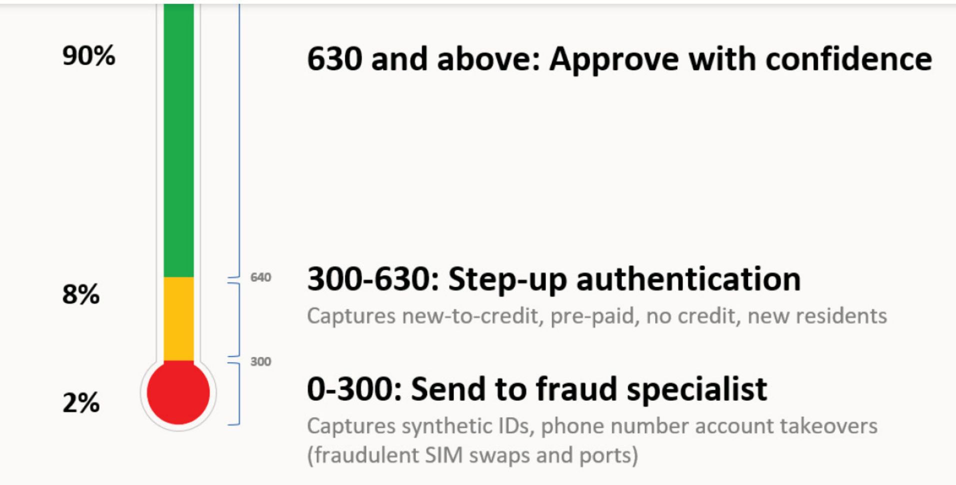
Exhibit 8 at 2.

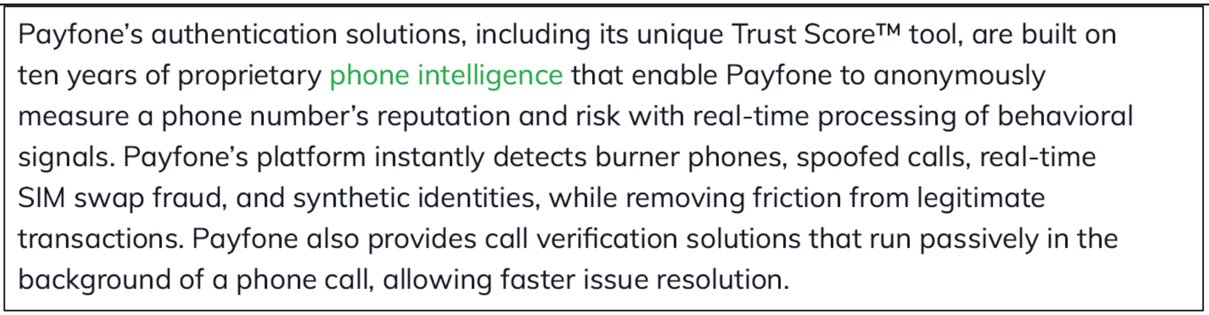
	 Instant Authentication for Voice **Description** Authenticates inbound call center calls and prevents ANI spoofing. **Solutions That Leverage This API** ○ Existing Customer Authentication ○ Fraud Prevention *Exhibit 8 at 4.*
(b) initiating a retrieval process to retrieve information associated with the phone number from a predetermined network location of a network authority, wherein the information is retrieved from a database storing phone numbers associated with a plurality of end-user devices, and wherein an entity authorized with the network authority to use the phone number provides the information to the network authority to associate the information with the phone number; and	Prove's Call Center Authentication initiates a retrieval process to retrieve information associated with the phone number (e.g., ANI) from a predetermined network location of a network authority (e.g., Prove), wherein the information is retrieved from a database storing phone numbers associated with a plurality of end-user devices (e.g., Fonebook/Prove database), and wherein an entity authorized with the network authority (e.g., Prove) to use the phone number provides the information to the network authority to associate the information with the phone number.  Trust Score The Payfone Trust Score measures the potential risk associated with a digital identity, so you can trust that you know who your customers are. Payfone provides a real-time Trust Score, which validates a customer's identity and virtually eliminates impersonation attacks (for example, SIM swap fraud, account takeover, porting fraud and ANI-spoofing attacks.) In lieu of traditional authentication methods, which are static and hackable, the Trust Score analyzes billions of digital signals from multiple sources for a holistic, real-time measure of identity trust. The Trust Score lets businesses confidently service customers and promote new offers. *Exhibit 17 at 3.*

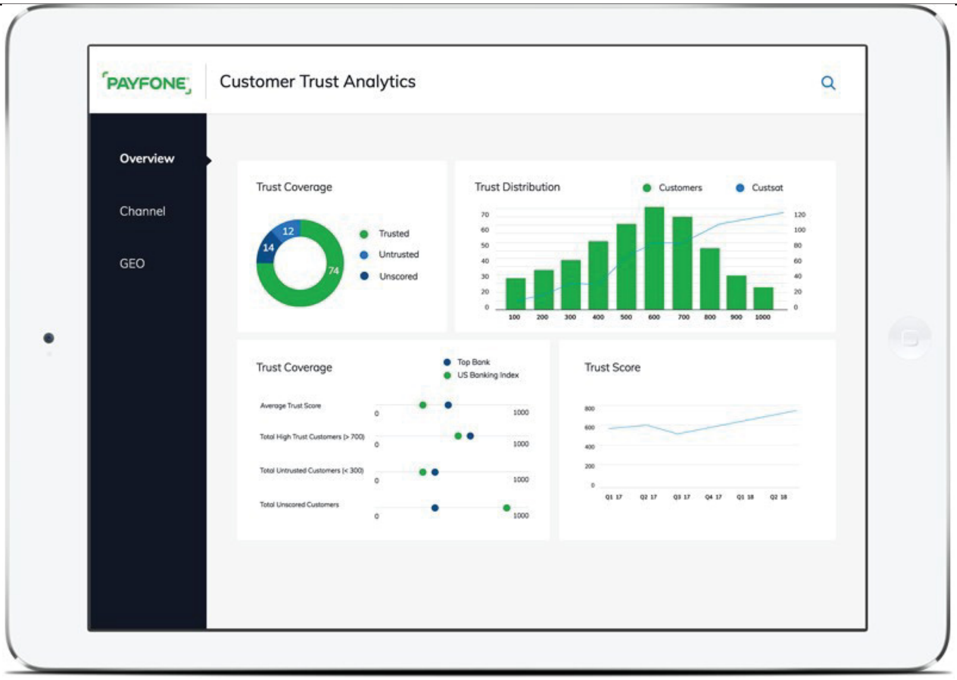
	 Fonebook **Description** Enables you to continuously update your customer records against millions of daily change events. Establishes persistent, private IDs for your customers so that their identities can be securely verified during interactions such as mobile and web logins, and call center calls. **Solutions That Leverage This API** ○ Account Opening ○ Existing Customer Authentication ○ Fraud Prevention *Exhibit 8 at 2.*

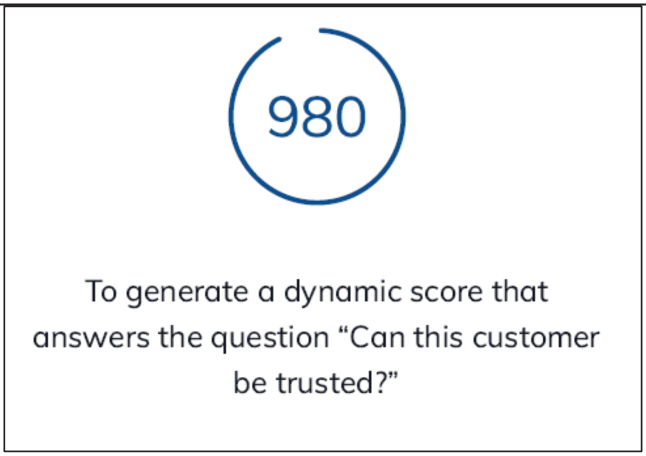
	 The call center is one of the most challenging channels when it comes to balancing security with customer experience. Fraud methods that target the call center – such as ANI-spoofing and account takeover attacks – are on the rise, with 51 percent of financial service professionals believing that phone channels see the greatest number of ATO attempts.* At the same time, we all know how unpleasant it can be to deal with security processes such as knowledge-based authentication and PIN codes when dialing into a call center, and quick and easy user enrollment remains a top priority for 91 percent of call center industry leaders.* The good news is that there is hope for brands looking to use technology to solve these issues. Payfone's Call Center solution uses a sophisticated, multi-layer approach to authenticating call center calls and the identity of callers to prevent ANI-spoofing and ATOs while also delivering a frictionless experience to >90% of callers. Enterprises can alleviate security concerns by leveraging the Payfone Trust Score™ and call authentication for real-time porting and SIM swap intelligence and to prove possession of the phone dialing into the call center. The Fonebook can then be used to identify callers for an increased ANI-match rate that eliminates the need for KBA questions and contains callers in the IVR so that they can quickly service themselves instead of requiring human intervention. *Exhibit 10 at 1.*

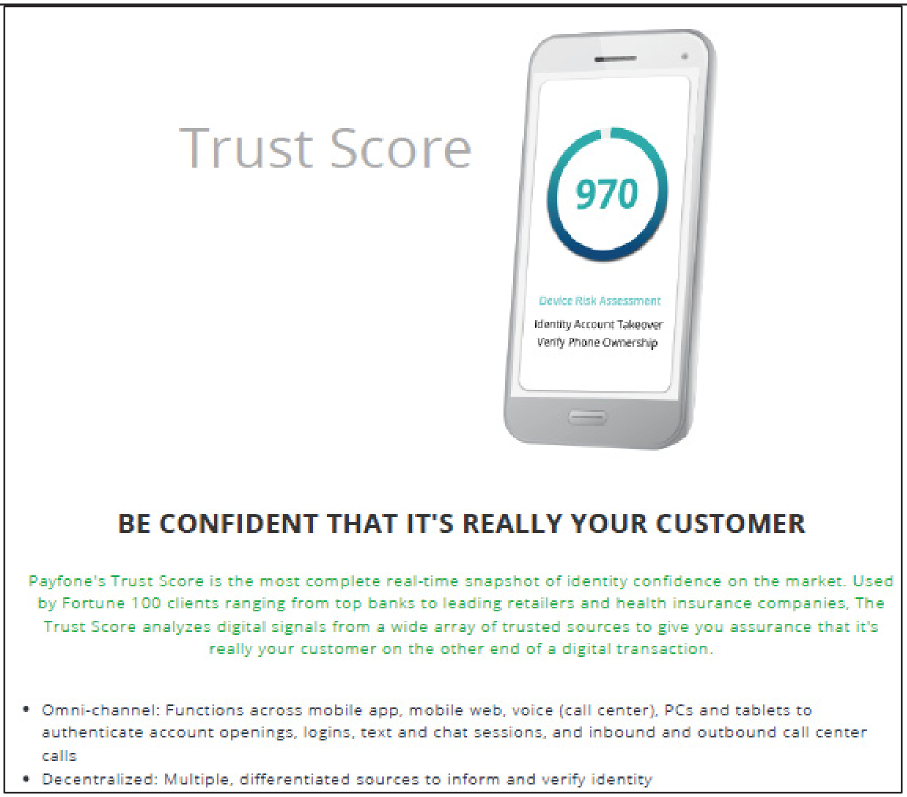
	 Trust Score 970 Device Risk Assessment Identity Account Takeover Verify Phone Ownership **BE CONFIDENT THAT IT'S REALLY YOUR CUSTOMER** Payfone's Trust Score is the most complete real-time snapshot of identity confidence on the market. Used by Fortune 100 clients ranging from top banks to leading retailers and health insurance companies, The Trust Score analyzes digital signals from a wide array of trusted sources to give you assurance that it's really your customer on the other end of a digital transaction. • Omni-channel: Functions across mobile app, mobile web, voice (call center), PCs and tablets to authenticate account openings, logins, text and chat sessions, and inbound and outbound call center calls • Decentralized: Multiple, differentiated sources to inform and verify identity *Exhibit 14 at 1.* Rodger Desai indicated that Prove analyzes information such as tenure of a number, behavior, and funding mechanism. *See* Consult Hyperion: Event 21 - Fireside Chat With Rodger Desai, *available at* https://chyp.com/webinars/week-21-fireside-chat-with-rodger-desai/; *see also* Payfone's Rodger Desai: Digital Transactions Should Be As Easy As Making A Phone Call, *available at https://tearsheet.co/podcasts/payfones-rodger-desai-digital-transactions-should-be-as-easy-as-making-a-phone-call/*

(c) rendering the retrieved information and the phone number of the incoming communication using the computing device.	Prove's Call Center Authentication renders (e.g., generates a Trust Score) the retrieved information and the phone number of the incoming communication using the computing device.  Leveraging Payfone's ecosystem of authoritative identity verifiers, the Trust Platform confidently and quickly confirms digital identities and closes the '**Trust Gap**' between companies and their customers. The Trust Platform allows companies to beat fraudsters, protect consumer privacy and deliver a VIP express lane customer experience for over 90% of interactions. **Trust Score™** The Payfone **Trust Score** analyzes real-time digital signals to generate a dynamic score that enables businesses to instantly and confidently answer the question "Should I trust this interaction?" *Exhibit 11 at 4.*  **630 and above: Approve with confidence** **300-630: Step-up authentication** Captures new-to-credit, pre-paid, no credit, new residents **0-300: Send to fraud specialist** Captures synthetic IDs, phone number account takeovers (fraudulent SIM swaps and ports) *Exhibit 11 at 5.*

	 Payfone’s authentication solutions, including its unique Trust Score™ tool, are built on ten years of proprietary phone intelligence that enable Payfone to anonymously measure a phone number’s reputation and risk with real-time processing of behavioral signals. Payfone’s platform instantly detects burner phones, spoofed calls, real-time SIM swap fraud, and synthetic identities, while removing friction from legitimate transactions. Payfone also provides call verification solutions that run passively in the background of a phone call, allowing faster issue resolution. *Exhibit 15 at 2.*

	 PAYFONE Customer Trust Analytics Overview Channel GEO Trust Coverage 12 14 74 Trusted Untrusted Unscored Trust Distribution Customers Custsat 70 60 50 40 30 20 0 120 100 80 60 40 20 0 100 200 300 400 500 600 700 800 900 1000 Trust Coverage Top Bank US Banking Index Average Trust Score Total High Trust Customers (> 700) Total Untrusted Customers (< 300) Total Unscored Customers 0 1000 Trust Score 800 600 400 200 0 Q1 17 Q2 17 Q3 17 Q4 17 Q1 18 Q2 18 *Exhibit 20 at 1.*

	 980 To generate a dynamic score that answers the question “Can this customer be trusted?” *Exhibit 17 at 3.*

	 970 Device Risk Assessment Identity Account Takeover Verify Phone Ownership Trust Score **BE CONFIDENT THAT IT'S REALLY YOUR CUSTOMER** Payfone's Trust Score is the most complete real-time snapshot of identity confidence on the market. Used by Fortune 100 clients ranging from top banks to leading retailers and health insurance companies. The Trust Score analyzes digital signals from a wide array of trusted sources to give you assurance that it's really your customer on the other end of a digital transaction. • Omni-channel: Functions across mobile app, mobile web, voice (call center), PCs and tablets to authenticate account openings, logins, text and chat sessions, and inbound and outbound call center calls • Decentralized: Multiple, differentiated sources to inform and verify identity *Exhibit 14 at 1.*